

# **Attachment 4-2-1**

## **WiMAX Forum<sup>®</sup> Network Architecture**

### **Detailed Protocols and Procedures**

Base Specification

**WMF-T33-001-R015v01**

**Note:** This Document is reproduced without any modification with the consent of the WiMAX Forum®, which owns the copyright in them.





# **WiMAX Forum<sup>®</sup> Network Architecture**

Detailed Protocols and Procedures

Base Specification

**WMF-T33-001-R015v01**

WiMAX Forum<sup>®</sup> Approved

(2009-11-21)

**WiMAX Forum Proprietary**

**Copyright © 2007-2009 WiMAX Forum. All Rights Reserved.**





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

Copyright 2007-2009 WiMAX Forum. All rights reserved.

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

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

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

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

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

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

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

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

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

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

“WiMAX,” “Mobile WiMAX,” “Fixed WiMAX,” “WiMAX Forum,” “WiMAX Certified,” “WiMAX Forum Certified,” the WiMAX Forum logo and the WiMAX Forum Certified logo are trademarks of the WiMAX Forum. Third-party trademarks contained in this document are the property of their respective owners.

## Table of Contents

1.	INTRODUCTION AND SCOPE.....	1
1.1	Relationship between Stage 2 and Stage 3 .....	1
1.2	Scope .....	1
1.3	Terminology .....	1
1.3.1	Terms .....	1
1.3.2	Conventions.....	1
2.	REFERENCES.....	2
3.	COMMONALITIES OF THE ASN CONTROL PROTOCOL.....	6
3.1	Encoding and Decoding.....	6
3.2	Message Header and Body .....	6
3.2.1	Usage of Source Identifier and Destination Identifier TLV.....	10
3.2.2	Transport Protocol Usage.....	11
3.3	Transport Protocol .....	11
3.4	Transport Requirements .....	12
3.4.1	Reliable Message Delivery.....	12
3.4.2	Message Size and Fragmentation.....	12
3.4.3	ASN Bearer Plane MTU Size.....	12
3.5	Error Handling and handling of unknown and inopportune control information .....	13
3.5.1	Handling of erroneous, unknown and inopportune control information by the receiver .....	13
3.5.1.1	Initial actions on an incoming control message .....	13
3.5.1.2	Subsequent error diagnostics .....	15
3.5.1.3	Actions when an error has been diagnosed .....	16
3.5.1.4	Subsequent handling of abnormal cases in the message flow of transactions .....	17
3.5.2	Error reporting.....	17
3.5.3	Reaction on receipt of an error report .....	18
3.5.4	Asynchronous Error Indication to Peers.....	19
4.	CONTROL PLANE PROTOCOLS AND PROCEDURES .....	20
4.1	Network Entry Discovery and Selection/Re-selection.....	20
4.1.1	General.....	20
4.1.2	Detailed Procedure .....	20
4.1.2.1	NAP Discovery .....	20
4.1.2.2	NSP Discovery.....	20
4.1.2.3	NSP Enumeration and Selection.....	23
4.1.2.3.1	Manual Mode .....	24
4.1.2.3.2	Automatic Mode.....	24
4.1.2.4	ASN Attachment.....	24
4.1.3	Configuration Information .....	25
4.1.4	SDL.....	27
4.1.4.1	Process Flow Descriptions .....	29
4.2	IP Addressing .....	32
4.2.1	IPv4 Addressing .....	32
4.2.2	IPv6 Addressing .....	32
4.3	WiMAX Key Hierarchy and Distribution .....	32
4.3.1	Mobile IP Root Key (MIP- RK).....	34
4.3.1.1	Key Generation .....	34
4.3.1.1.1	Collision Prevention for SPI Values.....	35
4.3.1.2	Key Distribution .....	36

1	4.3.1.3	Key Deprecation .....	37
2	4.3.2	AK Key .....	38
3	4.3.2.1	Key Generation .....	38
4	4.3.2.2	Key Lifetime .....	38
5	4.3.3	AK SN, PMK SN Usage and AK Context .....	38
6	4.3.3.1	Clarification of AK SN and PMK SN .....	38
7	4.3.3.2	PMK SN Usage in Initial Authentication .....	38
8	4.3.3.3	PMK SN Usage in Re-authentication .....	38
9	4.3.3.4	AK SN Derivation from PMK SN .....	38
10	4.3.4	CMAC Keys and Replay Protection for Management Messages .....	39
11	4.3.4.1	Maintenance of CMAC_KEY_COUNT <sub>TM</sub> by MS .....	39
12	4.3.4.1.1	CMAC_Key_Count_Lock and CMAC_Key_Count_Unlock States .....	39
13	4.3.4.2	Maintenance of CMAC_KEY_COUNT by the Network .....	39
14	4.3.4.2.1	Processing of CMAC_KEY_COUNT by the BS .....	39
15	4.3.4.2.2	Processing of CMAC_KEY_COUNT by the Anchor Authenticator .....	40
16	4.3.4.3	Implications for Various Handover and Re-entry Scenarios .....	41
17	4.3.4.3.1	Handover Cancellation .....	41
18	4.3.4.3.2	Handover Failure .....	41
19	4.3.4.4	Process Flowchart .....	41
20	4.3.5	MIP Keys .....	42
21	4.3.5.1	Key Generation .....	43
22	4.3.5.2	Key Generation Example .....	45
23	4.3.5.3	Key Distribution .....	45
24	4.3.5.3.1	Key Distribution for CMIP4 .....	46
25	4.3.5.3.2	Key Distribution for PMIP4 .....	48
26	4.3.5.3.3	Key Distribution for CMIP6 .....	49
27	4.3.5.3.4	Key Distribution for PMIP6 .....	50
28	4.3.5.4	Key Lifetime .....	51
29	4.3.6	DHCP keys .....	51
30	4.3.6.1	Key Generation .....	51
31	4.3.6.2	Key Distribution .....	52
32	4.4	Authentication, Authorization and Accounting .....	55
33	4.4.1	Network Access Authentication and Authorization .....	55
34	4.4.1.1	Network Access Authentication Model .....	56
35	4.4.1.2	EAP Methods .....	56
36	4.4.1.2.1	EAP-TLS .....	56
37	4.4.1.2.2	EAP-AKA .....	57
38	4.4.1.2.3	EAP-TTLS .....	57
39	4.4.1.3	Network Access Identifier .....	58
40	4.4.1.3.1	Outer-Identity .....	58
41	4.4.1.4	Detailed Impact on Functional Entities .....	60
42	4.4.1.4.1	MS Requirements .....	60
43	4.4.1.4.2	NAS Requirements .....	62
44	4.4.1.4.3	Visited CSN AAA Requirements .....	66
45	4.4.1.4.4	Home CSN AAA Requirements .....	67
46	4.4.1.5	Reauthentication .....	70
47	4.4.1.5.1	Reauthentication Triggers .....	70
48	4.4.1.5.2	Reauthentication Process .....	71
49	4.4.1.5.3	Management of PMK SN During Reauthentication .....	72
50	4.4.1.5.4	Reauthentication Process Without Authenticator Relocation .....	73
51	4.4.1.5.5	Reauthentication with Authenticator Relocation or Authenticator and FA Relocation .....	80
52	4.4.1.5.6	Error Handling During Reauthentication .....	97
53	4.4.1.6	Network Service Capability Negotiation and Authorization .....	99
54	4.4.1.6.1	NAS Requirement for Network Service Capability Negotiation .....	100
55	4.4.1.6.2	VCSN Requirement for Network Service Capability Negotiation .....	101
56	4.4.1.6.3	HCSN Requirement for Network Service Capability Negotiation .....	102

1	4.4.2	EAP Authentication Relay .....	102
2	4.4.3	Accounting.....	103
3	4.4.3.1	Introduction.....	103
4	4.4.3.2	Accounting Modes and Terminology .....	104
5	4.4.3.3	On-line Accounting (Prepaid Services) .....	105
6	4.4.3.3.1	RADIUS based Procedures .....	105
7	4.4.3.3.2	Diameter based Procedures .....	107
8	4.4.3.3.3	Accounting Information Collection and UDR Structure .....	110
9	4.4.3.3.4	Tariff Switching .....	110
10	4.4.3.3.5	PPC Relocation in case of RADIUS based Online Accounting .....	110
11	4.4.3.3.6	PPC Relocation in case of Diameter based Online Accounting .....	112
12	4.4.3.3.7	PPA Relocation .....	115
13	4.4.3.3.8	PPA-PPC quota(s) update.....	117
14	4.4.3.4	Offline (Post-Paid) Accounting .....	119
15	4.4.3.4.1	Concept.....	119
16	4.4.3.4.2	Protocol .....	122
17	4.4.3.4.3	Accounting Information Collection and UDR Structure .....	124
18	4.4.3.4.4	Procedures .....	124
19	4.4.3.4.5	Tariff Switching .....	126
20	4.4.3.4.6	Accounting R4 Messaging .....	126
21	4.4.3.4.7	Accounting Client Relocation .....	130
22	4.4.3.5	Hot-lining.....	133
23	4.4.3.5.1	Active Session Hot-lining.....	133
24	4.4.3.5.2	New IP Session Hot-lining .....	138
25	4.4.3.5.3	Hot-lining during initial network entry.....	140
26	4.4.3.5.4	Accounting Agent Relocation .....	141
27	4.4.3.5.5	Context update procedure for Hot-Lining .....	143
28	4.4.3.6	Accounting Messages .....	144
29	4.4.3.6.1	R6 Reference Point.....	144
30	4.4.3.6.2	R4 Reference Point.....	147
31	4.4.3.7	Accounting Events in the ASN .....	154
32	4.4.3.8	Accounting Events in the CSN .....	154
33	4.4.3.9	Illustrations of the Accounting Start Events in the ASN .....	155
34	4.4.3.10	Illustrations of the Accounting Start Events in the CSN.....	161
35	4.5	Network Entry and Exit .....	165
36	4.5.1	MS-to-Network Initial Authentication Flow .....	165
37	4.5.1.1	Single EAP.....	165
38	4.5.1.2	Error Handling During Initial Network Entry.....	177
39	4.5.1.2.1	Timers and Timing Considerations .....	177
40	4.5.1.2.2	Handling Error Conditions .....	178
41	4.5.1.2.3	Timer Expiry .....	179
42	4.5.1.2.4	Duplicate MAC address handling.....	179
43	4.5.1.3	Network Rejection Procedure .....	180
44	4.5.1.3.1	Network Rejection Information.....	186
45	4.5.1.3.2	Rejection Classes.....	186
46	4.5.2	Network Exiting.....	187
47	4.5.2.1	Normal Mode.....	188
48	4.5.2.1.1	MS Triggered Network Exit .....	189
49	4.5.2.1.2	Network Trigger .....	190
50	4.5.2.2	Idle Mode.....	199
51	4.5.2.2.1	MS Triggered Network Exit (Idle Mode).....	199
52	4.5.2.2.2	Network Trigger .....	200
53	4.5.2.3	Message Composition.....	204
54	4.5.2.3.1	R4/ R6 Data Path Control Messages .....	204
55	4.5.2.3.2	R4/R6 MS State Change Messages .....	205
56	4.5.2.3.3	R3 AAA Messages .....	206

1	4.5.2.4	Network Exiting Timers and Considerations .....	206
2	4.5.2.4.1	Timer Expiry .....	207
3	4.6	QoS and SFID Management .....	207
4	4.6.1	Introduction .....	207
5	4.6.2	Functional Model .....	208
6	4.6.2.1	Policy Framework .....	208
7	4.6.3	Subscriber QoS Profile .....	208
8	4.6.4	Service Flow Management .....	208
9	4.6.4.1	Pre-Provisioned Service Flows .....	209
10	4.6.4.1.1	Create Service Flow .....	209
11	4.6.4.1.2	Delete Service Flow .....	209
12	4.6.4.1.3	Modify Service Flow .....	209
13	4.6.4.2	Initial Service Flow .....	209
14	4.6.4.2.1	IP-CS Related Issues .....	210
15	4.6.4.2.2	Ethernet-CS Related Information .....	214
16	4.6.4.2.3	Common Issues .....	215
17	4.6.4.2.4	Create Service Flow .....	215
18	4.6.4.2.5	Delete Service Flow .....	215
19	4.6.4.2.6	Modify Service Flow .....	215
20	4.6.4.3	Dynamic Service Flows .....	215
21	4.6.4.3.1	Create Service Flow .....	216
22	4.6.4.3.2	Delete Service Flow .....	216
23	4.6.4.3.3	Modify Service Flow .....	216
24	4.6.4.4	Data Path Handling .....	216
25	4.6.4.5	Message Flows and Flow Description .....	217
26	4.6.4.5.1	Update of Pre-Provisioned QoS triggered by AAA .....	217
27	4.6.4.5.2	Network Initiated Service Flow Creation/Modification .....	218
28	4.6.4.5.3	MS Initiated Service Flow Creation .....	220
29	4.6.4.5.4	MS Initiated Service Flow Modification .....	222
30	4.6.4.5.5	Network Initiated Service Flow Deletion .....	223
31	4.6.4.5.6	MS Initiated Service Flow Deletion .....	225
32	4.6.4.5.7	SF Management Timers and Timing Considerations .....	226
33	4.6.4.5.8	SF Management Error Conditions .....	227
34	4.6.5	QoS Messages .....	228
35	4.6.5.1	Messages and Information Elements (IEs) for QoS control in the ASN .....	228
36	4.6.5.2	RR_Req .....	229
37	4.6.5.2.1	Service Flow Creation or Modification (Anchor-SFA to Serving-SFA) .....	229
38	4.6.5.2.2	Service Flow Creation (Serving-SFA to Anchor-SFA) .....	232
39	4.6.5.2.3	Service Flow Modification for state change (Serving-SFA to Anchor-SFA) .....	235
40	4.6.5.2.4	Service Flow Deletion .....	238
41	4.6.5.3	RR_Rsp .....	238
42	4.6.5.3.1	Service Flow Creation .....	238
43	4.6.5.3.2	Service Flow Deletion .....	240
44	4.6.5.3.3	RR_Ack .....	240
45	4.6.5.4	Combined Data Path and QoS Control Messages IEs .....	240
46	4.6.5.4.1	Combined Service Flow Creation .....	240
47	4.6.5.4.2	Combined Service Flow Modification .....	254
48	4.6.5.4.3	In Case of Modification of a SF and the Related DP .....	254
49	4.6.5.4.4	Combined Service Flow Deletion .....	261
50	4.6.6	SFID Management .....	262
51	4.6.7	QoS Profile in the MS .....	262
52	4.7	ASN Anchored Mobility .....	263
53	4.7.1	Introduction .....	263
54	4.7.2	Fully Controlled HO .....	264
55	4.7.2.1	HO Preparation Phase .....	264

1	4.7.2.1.1 Handover Preparation Scenario 1: AK Context Retrieval and Path Pre-Registration Initiated by Target BS.....	265
2	4.7.2.1.2 Handover Preparation Scenario 2: AK Context sent by Serving ASN-GW and Path Pre-Registration Initiated by Target ASN-GW .....	267
3	4.7.2.1.3 Handover Preparation Scenario 3: Anchor ASN-GW Collocated with Serving ASN-GW and Path Pre-Registration Piggybacked onto HO Control messages.....	269
4	4.7.2.1.4 MS-Initiated HO Preparation Phase – Co-located Serving, Relay and Authenticator ASN-GW (Scenario 6).....	273
5	4.7.2.1.5 Network Initiated HO Scenarios.....	274
6	4.7.2.1.6 HO Preparation Stage Timers and Timing Considerations.....	276
7	4.7.2.1.7 HO Preparation Stage Error Conditions .....	277
8	4.7.2.2 HO Action Phase .....	278
9	4.7.2.2.1 Handover Action Scenario 1: Serving BS Sends HO_Cnf to Target BS .....	280
10	4.7.2.2.2 Handover Action Scenario 2: HO_Cnf not Received at Target BS.....	283
11	4.7.2.2.3 Handover Action Scenario 3: MOB_HO-IND not received at Serving BS.....	285
12	4.7.2.2.4 Handover Action Scenario 4: Anchor ASN-GW and Anchor Authenticator Collocated with Serving ASN-GW – Serving ASN-GW Initiates Path Registration .....	288
13	4.7.2.3 HO Cancellation .....	291
14	4.7.2.3.1 HO Cancellation Scenario 1: Serving and Anchor ASN-GW are Collocated and “Unselected Target BS” Receives HO_Cnf from Serving BS .....	292
15	4.7.2.3.2 HO Cancellation Scenario 2: Serving and Anchor ASN-GW are not Collocated and “Unselected Target BS” receives HO_Cnf from Serving BS .....	293
16	4.7.2.3.3 HO Cancellation Scenario 3: A subset of the Target BS(s) does not Receive HO_Cnf(Cancel). 294	
17	4.7.2.3.4 HO Cancellation Scenario 4: Serving BS receives HO_Complete.....	295
18	4.7.2.4 MS Handover Rejection.....	296
19	4.7.2.5 HO Action Phase Timers and Timing Considerations .....	296
20	4.7.2.6 HO Action Phase Error Conditions.....	298
21	4.7.2.6.1 Timer Expiry .....	298
22	4.7.2.6.2 Path_Reg_Rsp Error.....	299
23	4.7.2.6.3 HO_Cnf Error.....	299
24	4.7.3 Uncontrolled (Unpredictive) HO with Context Retrieval.....	299
25	4.7.3.1 Successful Uncontrolled Handover.....	300
26	4.7.4 HO and Scanning Control for Fixed/Nomadic SS/MS.....	302
27	4.7.5 Message Definitions for HO Preparation Phase.....	303
28	4.7.5.1 Message Definitions for HO Preparation Phase.....	303
29	4.7.5.2 Message Definitions for HO Action Phase .....	318
30	4.7.6 ASN Anchored Mobility Scenarios Over R8 and R6 .....	338
31	4.7.6.1 Fully Controlled HO .....	339
32	4.7.6.1.1 HO Preparation Phase.....	339
33	4.7.6.1.2 HO Action Phase .....	343
34	4.7.6.1.3 HO Cancel .....	351
35	4.7.6.1.4 HO Reject.....	353
36	4.7.6.2 Uncontrolled HO.....	354
37	4.7.6.3 Message Definitions .....	356
38	4.7.7 Data Integrity .....	356
39	4.7.7.1 Introduction.....	356
40	4.7.7.2 Data Paths during handover .....	356
41	4.7.7.3 Data Integrity without ARQ Synchronization.....	357
42	4.7.7.3.1 Downlink Data Integrity Methods .....	357
43	4.7.7.3.2 Uplink Data Integrity.....	368
44	4.7.7.3.3 Auxiliary Use of SDU SN Report .....	368
45	4.7.7.3.4 Informational Elements Added by this Functionality.....	369
46	4.7.7.4 Data Integrity with ARQ Synchronization.....	372
47	4.7.7.4.1 Synchronization of ARQ State .....	372
48	4.7.7.4.2 Downlink Data Integrity Methods.....	377

1	4.7.7.4.3	Uplink Data Integrity Methods .....	378
2	4.7.7.4.4	Auxiliary Use of SDU SN Report .....	384
3	4.7.7.4.5	Informational Elements Added by this Functionality .....	384
4	4.7.7.5	Negotiating Data Integrity Method .....	385
5	4.8	CSN Anchored Mobility Management .....	387
6	4.8.1	Introduction.....	387
7	4.8.2	Proxy MIP4 R3 Mobility Management.....	388
8	4.8.2.1	Proxy MIP4 Connection Setup Procedure .....	388
9	4.8.2.1.1	MS Requirements .....	388
10	4.8.2.1.2	DHCP proxy/relay/server Requirements .....	388
11	4.8.2.1.3	PMIP4 Client Requirements .....	392
12	4.8.2.1.4	FA Requirements.....	392
13	4.8.2.1.5	HA Requirements .....	393
14	4.8.2.1.6	AAA Server Requirements.....	396
15	4.8.2.1.7	PMIP4 Connection Setup Call Flow .....	398
16	4.8.2.2	Proxy MIP4 Session Renewal Procedure.....	405
17	4.8.2.2.1	MS Requirements .....	406
18	4.8.2.2.2	DHCP Requirements .....	406
19	4.8.2.2.3	PMIP4 Client Requirements .....	407
20	4.8.2.2.4	FA Requirements.....	407
21	4.8.2.2.5	HA Requirements .....	407
22	4.8.2.2.6	AAA Server Requirements.....	407
23	4.8.2.2.7	PMIP4 Session Renewal Call Flows .....	407
24	4.8.2.3	Proxy MIP4 CSN Anchored Mobility Handover .....	409
25	4.8.2.3.1	MS Requirements .....	413
26	4.8.2.3.2	DHCP Proxy/Relay Requirements .....	413
27	4.8.2.3.3	PMIP4 Client Requirements .....	414
28	4.8.2.3.4	FA Requirements.....	415
29	4.8.2.3.5	HA Requirements .....	415
30	4.8.2.3.6	AAA Server Requirements.....	415
31	4.8.2.3.7	PMIP4 Mobility Procedure.....	416
32	4.8.2.4	Proxy MIP4 Session Termination .....	419
33	4.8.2.4.1	MS Requirements .....	419
34	4.8.2.4.2	DHCP Requirements .....	419
35	4.8.2.4.3	PMIP4 Client Requirements .....	419
36	4.8.2.4.4	FA Requirements.....	420
37	4.8.2.4.5	HA Requirements .....	420
38	4.8.2.4.6	AAA Server Requirements.....	420
39	4.8.2.4.7	PMIP4 Session Release Procedure .....	420
40	4.8.2.5	Proxy MIP4 R3 Mobility Management for MIP-based Ethernet Services.....	426
41	4.8.2.5.1	Connection Setup Phase for MIP-based Ethernet Services .....	426
42	4.8.2.5.2	Session Renewal for Ethernet Services .....	428
43	4.8.2.5.3	CSN-anchored Mobility Management Handover for MIP-based Ethernet Services .....	428
44	4.8.2.5.4	Session Termination for Ethernet Services.....	429
45	4.8.2.5.5	Data plane handling .....	429
46	4.8.3	Client MIP4 R3 Mobility Management .....	429
47	4.8.3.1	Client MIP4 Connection Setup Procedure .....	430
48	4.8.3.1.1	MS Requirements .....	430
49	4.8.3.1.2	FA Requirements.....	431
50	4.8.3.1.3	HA Requirements .....	432
51	4.8.3.1.4	AAA Server Requirements.....	432
52	4.8.3.2	Client MIP4 Session Renewal .....	432
53	4.8.3.2.1	CMIP4 Session Renewal Procedure .....	432
54	4.8.3.3	Client MIP4 CSN Anchored Mobility Handover.....	432
55	4.8.3.3.1	MS Requirements .....	433
56	4.8.3.3.2	FA Requirements.....	433

1	4.8.3.3.3	HA Requirements .....	434
2	4.8.3.3.4	AAA Server Requirements .....	434
3	4.8.3.3.5	MS Mobility Triggered.....	434
4	4.8.3.3.6	Network Resource Optimization Triggered.....	434
5	4.8.3.3.7	CMIP4 Mobility Procedure .....	435
6	4.8.3.4	Client MIP4 Session Termination.....	437
7	4.8.3.4.1	MS Requirements .....	437
8	4.8.3.4.2	FA Requirements.....	438
9	4.8.3.4.3	HA Requirements .....	438
10	4.8.3.4.4	AAA Server Requirements .....	438
11	4.8.4	<i>Client MIP6 Mobility Management</i> .....	438
12	4.8.4.1	Client MIP6 Connection Setup Procedure .....	438
13	4.8.4.1.1	MS/CMIP6 Client Operation.....	440
14	4.8.4.1.2	NAS and DHCPv6 Proxy Requirements .....	441
15	4.8.4.1.3	HA Requirements .....	441
16	4.8.4.1.4	AAA Requirements and Behavior .....	442
17	4.8.4.2	MIP6 Inter Access Router (AR) Handovers .....	443
18	4.8.4.2.1	MS/ CMIP6 Client Operation.....	445
19	4.8.4.2.2	AR/NAS and DHCPv6 Proxy Operation.....	446
20	4.8.4.2.3	HA Behavior.....	446
21	4.8.4.2.4	AAA Requirements .....	447
22	4.8.4.3	MIP6 Session Renewal .....	447
23	4.8.4.3.1	MS/ CMIP6 Client Requirements.....	447
24	4.8.4.3.2	AR/ and DHCPv6 Proxy Requirements .....	447
25	4.8.4.3.3	HA Requirements .....	447
26	4.8.4.3.4	AAA Requirements .....	447
27	4.8.4.4	MIP6 Session Termination .....	447
28	4.8.4.4.1	MS/ CMIP6 Client Requirements.....	447
29	4.8.4.4.2	AR/NAS and DHCPv6 Proxy Requirements .....	447
30	4.8.4.4.3	HA Requirements .....	447
31	4.8.4.4.4	AAA Requirements .....	448
32	4.8.5	<i>Proxy MIP6 R3 Mobility Management</i> .....	448
33	4.8.5.1	PMIP6 Security.....	448
34	4.8.5.2	Management of IPv6 and IPv4 support.....	449
35	4.8.5.3	PMIP6 Connection Setup Procedure.....	450
36	4.8.5.3.1	MS Requirements .....	450
37	4.8.5.3.2	AAA/NAS Requirements .....	450
38	4.8.5.3.3	AR/MAG Requirements .....	451
39	4.8.5.3.4	DHCP Proxy/Relay Requirements .....	452
40	4.8.5.3.5	LMA Requirements .....	452
41	4.8.5.3.6	PMIP6 Connection Setup flows .....	453
42	4.8.5.4	PMIP6 Session Renewal Procedure.....	459
43	4.8.5.4.1	DHCP Renewal .....	459
44	4.8.5.4.2	PMIP6 Lifetime Renewal .....	459
45	4.8.5.5	PMIP6 CSN Anchored Mobility Handover .....	460
46	4.8.5.5.1	MS Requirements .....	460
47	4.8.5.5.2	Authenticator and AAA Server Requirements .....	460
48	4.8.5.5.3	AR/MAG Requirements .....	461
49	4.8.5.5.4	LMA Requirements .....	462
50	4.8.5.5.5	DHCP Requirements .....	462
51	4.8.5.5.6	PMIP6 CSN MM Flow(s) .....	462
52	4.8.5.5.7	Handover timers and timer considerations .....	468
53	4.8.5.5.8	Handover error conditions and recovery .....	469
54	4.8.5.6	PMIP6 Session Termination .....	470
55	4.8.5.6.1	AAA/NAS Requirements .....	470
56	4.8.5.6.2	AR/MAG Requirements .....	470



1	4.8.5.6.3	LMA Requirements .....	470
2	4.8.5.6.4	DHCP Requirements .....	470
3	4.8.5.6.5	PMIP6 Session Termination Flows .....	471
4	4.8.5.6.6	Handover timers and timer considerations .....	473
5	4.8.5.6.7	Handover error conditions and recovery .....	473
6	4.9	Radio Resource Management .....	473
7	4.9.1	Introduction.....	473
8	4.9.2	RRM Primitives and their Mapping to Reference Points .....	474
9	4.9.3	RRM Signaling .....	475
10	4.9.3.1	Per-BS Spare Capacity Reporting Procedure.....	475
11	4.9.3.1.1	Per-BS Spare Capacity Reporting Procedure with R6/R4 .....	475
12	4.9.3.1.2	Per-BS Spare Capacity Reporting Procedures with R8 .....	477
13	4.9.3.1.3	R4/R6/R8 Messages for Per-BS Capacity Reporting Procedures.....	478
14	4.9.3.2	Per-BS Radio Configuration Update Procedure .....	480
15	4.9.3.2.1	Per-BS Radio Configuration Update Procedure with R6/R4.....	480
16	4.9.3.2.2	Per-BS Radio Configuration Update Procedure with R8 .....	482
17	4.9.3.2.3	R4/R6/R8 Messages for Per-BS Radio Configuration Update Procedure .....	483
18	4.9.3.2.4	Radio Configuration Update Procedure Timers and Timing Considerations .....	485
19	4.10	Paging and Idle-Mode MS Operation.....	486
20	4.10.1	Introduction.....	486
21	4.10.2	Location Update.....	486
22	4.10.2.1	Successful Secure Location Update - No Paging Controller Relocation .....	486
23	4.10.2.2	Successful Secure Location Update with PC Relocation.....	489
24	4.10.2.3	Location Update Timers and Considerations .....	491
25	4.10.2.4	Location Update Error Procedures.....	492
26	4.10.2.4.1	Timer MAX Retries.....	492
27	4.10.2.4.2	Authenticator Context Retrieval failure.....	493
28	4.10.2.4.3	PC Relocation Failure.....	493
29	4.10.2.4.4	Secure Location Update Failure .....	493
30	4.10.2.4.5	CMAC Key Count Update Failure .....	493
31	4.10.2.4.6	Location Update out of MS Reattachment Zone .....	493
32	4.10.2.5	Location Update Message Tables .....	494
33	4.10.3	Paging Procedure.....	497
34	4.10.3.1	Topologically Aware Paging .....	498
35	4.10.3.2	Topologically Unaware Paging Scheme .....	498
36	4.10.3.3	Single-step vs. Multi-step Paging Operations.....	499
37	4.10.3.4	IP Multicasting Support for Paging_Announce .....	500
38	4.10.3.5	Paging Procedure Message Flow .....	500
39	4.10.3.6	Stop Paging Procedure.....	502
40	4.10.3.7	Paging Timers and Timing Considerations.....	504
41	4.10.3.8	Paging Error Conditions .....	504
42	4.10.3.8.1	Timer Expiry .....	504
43	4.10.3.8.2	R4 Initiate_Paging_Rsp.....	505
44	4.10.3.9	Messages for Paging Procedure .....	505
45	4.10.4	Idle Mode Exit .....	509
46	4.10.4.1	Idle Mode Exit – Serving ASN Does Not Have MS Context .....	509
47	4.10.4.1.1	Timers and Timing Considerations .....	511
48	4.10.4.1.2	Idle Mode Exit Error Conditions .....	512
49	4.10.4.2	Idle Mode Exit – Serving ASN Has MS Context .....	513
50	4.10.4.2.1	Timers and Timing Considerations .....	515
51	4.10.4.2.2	Fast Idle Mode Exit Error Conditions .....	516
52	4.10.4.3	IM Exit Message Tables .....	516
53	4.10.5	Idle Mode Entry.....	534
54	4.10.5.1	MS Initiated Idle Mode Entry .....	535
55	4.10.5.2	Network Initiated Idle Mode Entry.....	538
56	4.10.5.3	Idle Mode Entry Timers and Timing Considerations: .....	540

1	4.10.5.4	Idle Mode Entry Error Conditions .....	541
2	4.10.5.5	Timer Max Retries .....	541
3	4.10.5.6	AK Context Generation Error .....	542
4	4.10.5.7	R6 Data Path Deregistration Error .....	542
5	4.10.5.8	R4 Data Path Deregistration Error .....	542
6	4.10.5.9	IM Entry Message Tables .....	543
7	4.10.6	<i>Idle Mode Operation and CSN Anchored Mobility Management</i> .....	560
8	4.10.6.1	Anchor DPF and FA .....	560
9	4.10.6.2	CMIP in Idle Mode .....	561
10	4.10.6.2.1	FA Migration During Idle Mode: Anchor PC Initiated .....	561
11	4.10.6.2.2	FA Migration during Idle Mode: New (target) FA Initiated .....	565
12	4.10.6.3	PMIP4 in Idle Mode .....	567
13	4.10.6.3.1	PMIP4 in Idle Mode – FA Migration Triggered from the Anchor PC-ASN .....	568
14	4.10.6.3.2	PMIP4 in Idle Mode – FA Migration triggered from the Target ASN (New FA) .....	569
15	4.10.6.4	Idle Mode Operation and Simple IP Re-anchoring .....	569
16	4.10.6.4.1	Triggering Simple IP Re-anchoring .....	570
17	4.10.6.4.2	Simple IP Re-anchoring Procedure in Idle mode .....	570
18	4.10.6.5	PMIP6 in Idle Mode .....	571
19	4.11	IPv6 .....	573
20	4.11.1	<i>Network Model</i> .....	573
21	4.11.2	<i>Point to Point Link Between the MS and AR</i> .....	574
22	4.11.3	<i>IPv6 Link Establishment</i> .....	574
23	4.11.4	<i>Address Configuration</i> .....	575
24	4.11.4.1	Interface Identifier (IID) .....	575
25	4.11.4.2	Duplicate Address Detection (DAD) .....	576
26	4.11.4.3	Stateless Address Auto-configuration .....	576
27	4.11.4.4	Stateful Address Auto-configuration .....	576
28	4.11.5	<i>DNS Discovery</i> .....	576
29	4.11.5.1	DHCPv6 DNS Configuration Options .....	576
30	4.11.6	<i>Uplink and Downlink Transmission of IPv6 Packets</i> .....	577
31	4.11.6.1	Uplink .....	577
32	4.11.6.2	Downlink .....	577
33	4.11.7	<i>IPv6 AR Relocation (R3 relocation)</i> .....	577
34	4.12	Utility Call Flows .....	578
35	4.12.1	<i>Data Path Pre-Registration Procedure</i> .....	578
36	4.12.1.1	R4/R6 Data Path Pre-Registration Procedure .....	578
37	4.12.1.2	R6 Data Path Pre-Registration Procedure .....	579
38	4.12.2	<i>Context Retrieval Procedure</i> .....	580
39	4.12.2.1	R4/R6 Context Retrieval Procedure .....	580
40	4.12.2.2	R6 Context Retrieval Procedure .....	581
41	4.12.3	<i>Data Path Registration Procedure</i> .....	582
42	4.12.3.1	R4/R6 Data Path Registration Procedure .....	582
43	4.12.3.2	R6 Data Path Registration Procedure .....	583
44	4.12.4	<i>R4 Data Path De-Registration Procedure</i> .....	584
45	4.12.4.1	R4/R6 Data Path De-Registration Procedure .....	584
46	4.12.4.2	R6 Data Path De-Registration Procedure .....	585
47	4.12.5	<i>CMAC Key Count Update Procedure</i> .....	586
48	4.12.5.1	R4/R6 CMAC Key Count Update Procedure .....	586
49	4.12.5.2	R6 CMAC Key Count Update Procedure .....	587
50	4.12.6	<i>MAC Context Retrieval Procedure</i> .....	588
51	4.12.7	<i>EAP Notification Exchange</i> .....	589
52	4.13	Simple IP Management .....	590
53	4.13.1	<i>AR requirements</i> .....	590
54	4.13.2	<i>CR requirements</i> .....	590
55	4.13.3	<i>AAA server requirements</i> .....	591
56	4.13.4	<i>Requirements specific to Simple IPv4 service</i> .....	591

1	4.13.4.1	MS Requirements .....	591
2	4.13.4.2	DHCP Requirements.....	591
3	4.13.4.2.1	DHCP Proxy requirements .....	592
4	4.13.4.2.2	DHCP Relay requirements .....	592
5	4.13.4.2.3	DHCP server requirements .....	593
6	4.13.5	<i>Requirements specific to Simple IPv6 service</i> .....	593
7	4.13.5.1	MS Requirements .....	593
8	4.13.5.2	DHCPv6 Requirements.....	594
9	4.13.5.2.1	DHCPv6 proxy requirements .....	594
10	4.13.5.2.2	DHCPv6 relay requirements.....	594
11	4.13.5.2.3	DHCPv6 server requirements .....	594
12	4.13.5.3	AR Requirements.....	595
13	4.13.5.4	CR Requirements .....	595
14	4.14	Simple Ethernet Service Management.....	595
15	4.14.1	<i>MS requirement</i> .....	595
16	4.14.2	<i>L2 Forwarder (L2FW) requirements</i> .....	595
17	4.14.3	<i>Ethernet Service Core Bridge (eCB) requirements</i> .....	596
18	4.14.4	<i>AAA server requirements</i> .....	596
19	4.14.5	<i>Layer 2 DHCP Relay requirements</i> .....	596
20	4.15	Release and Capability Negotiation Function on R4/R6/R8 .....	597
21	4.15.1	<i>General</i> .....	597
22	4.15.2	<i>Procedure Specification</i> .....	598
23	4.15.3	<i>Message definitions</i> .....	600
24	4.16	R3-R5 Version Negotiation .....	602
25	4.16.1	<i>Version Alignment Between ASN-GW and HA</i> .....	604
26	4.16.2	<i>Requirements</i> .....	604
27	4.16.2.1	General Requirements.....	604
28	4.16.2.2	NAS Requirements .....	604
29	4.16.2.3	VAAA Requirements.....	605
30	4.16.2.4	HAAA Requirements.....	605
31	4.16.3	<i>Support for Release 1.0 VAAA</i> .....	606
32	4.17	Keep-alive mechanism .....	606
33	4.17.1	<i>Requirements</i> .....	609
34	4.17.1.1	Keep-alive Req Sender requirements.....	609
35	4.17.1.2	Keep-alive Req Receiver requirements.....	609
36	4.18	Application Server Discovery.....	610
37	4.18.1	<i>DHCP Proxy in the ASN</i> .....	610
38	4.18.2	<i>DHCP Relay in the ASN</i> .....	610
39	4.18.3	<i>Server Discovery for Roaming Users</i> .....	611
40	5.	MESSAGE AND PARAMETER DEFINITIONS.....	612
41	5.1	Constants and Counters .....	612
42	5.1.1	<i>CMAC_Key_Count Counter</i> .....	612
43	5.1.2	<i>CMAC Packet Number Counter</i> .....	612
44	5.1.3	<i>CMAC PN * Counter</i> .....	612
45	5.1.4	<i>Entry Counter</i> .....	612
46	5.1.5	<i>HO Req Retransmission Limit</i> .....	612
47	5.1.6	<i>R6 HO Req Retry Counter</i> .....	612
48	5.2	Message Definitions and Construction Rules.....	612
49	5.3	TLV Definitions .....	617
50	5.3.1	<i>TLV Format</i> .....	617
51	5.3.2	<i>TLV Encoding</i> .....	618
52	5.3.2.1	Accept/Reject Indicator .....	618
53	5.3.2.2	Accounting Extension.....	618
54	5.3.2.3	Action Code .....	619

1	5.3.2.4	Action Time .....	619
2	5.3.2.5	AK .....	619
3	5.3.2.6	AK Context .....	620
4	5.3.2.7	AK ID .....	620
5	5.3.2.8	AK Lifetime .....	620
6	5.3.2.9	AK SN .....	620
7	5.3.2.10	Anchor ASN GW ID.....	621
8	5.3.2.11	Anchor MM Context.....	621
9	5.3.2.12	Anchor PC ID .....	621
10	5.3.2.13	Anchor PC Relocation Destination .....	622
11	5.3.2.14	Anchor PC Relocation Request Response .....	622
12	5.3.2.15	Associated PHSI .....	622
13	5.3.2.16	FA Revoke Reason .....	623
14	5.3.2.17	Authentication Complete .....	623
15	5.3.2.18	Authentication Result .....	623
16	5.3.2.19	Authenticator ID .....	624
17	5.3.2.20	RRQ .....	624
18	5.3.2.21	Authorization Policy Support .....	624
19	5.3.2.22	Available Radio Resource DL .....	625
20	5.3.2.23	Available Radio Resource UL .....	625
21	5.3.2.24	BE Data Delivery Service .....	626
22	5.3.2.25	BS ID .....	626
23	5.3.2.26	BS Info.....	627
24	5.3.2.27	BS-originated EAP-Start Flag.....	628
25	5.3.2.28	Care-of Address (CoA) .....	628
26	5.3.2.29	CID/MCID .....	628
27	5.3.2.30	Classification Rule Index .....	628
28	5.3.2.31	Classification Rule Action .....	629
29	5.3.2.32	Classification Rule Priority.....	629
30	5.3.2.33	Void .....	629
31	5.3.2.34	CMAC_KEY_COUNT.....	629
32	5.3.2.35	Combined Resources Required.....	630
33	5.3.2.36	Context Purpose Indicator.....	630
34	5.3.2.37	Correlation ID .....	631
35	5.3.2.38	Cryptographic Suite .....	632
36	5.3.2.39	CS Type .....	632
37	5.3.2.40	Data Integrity .....	633
38	5.3.2.41	PMIP-Authenticated-Network-Identity .....	633
39	5.3.2.42	Data Path Encapsulation Type .....	633
40	5.3.2.43	Void .....	633
41	5.3.2.44	Data Path ID .....	633
42	5.3.2.45	Data Path Info .....	634
43	5.3.2.46	Void .....	634
44	5.3.2.47	Data Path Type.....	634
45	5.3.2.48	DCD/UCD Configuration Change Count .....	634
46	5.3.2.49	DCD Setting.....	634
47	5.3.2.50	ODFMA Parameters Sets.....	635
48	5.3.2.51	DHCP Key .....	635
49	5.3.2.52	DHCP Key ID .....	636
50	5.3.2.53	DHCP Key Lifetime .....	636
51	5.3.2.54	DHCP Proxy Info.....	636
52	5.3.2.55	DHCP Relay Address .....	636
53	5.3.2.56	DHCP Relay Info .....	637
54	5.3.2.57	DHCP Server Address .....	637
55	5.3.2.58	DHCP Server List .....	637
56	5.3.2.59	Direction .....	638

1	5.3.2.60	DL PHY Quality Info .....	638
2	5.3.2.61	DL PHY Service Level .....	638
3	5.3.2.62	EAP Payload .....	638
4	5.3.2.63	Void .....	639
5	5.3.2.64	ERT-VR Data Delivery Service.....	639
6	5.3.2.65	PPAC .....	639
7	5.3.2.66	FA-HA Key .....	640
8	5.3.2.67	FA-HA Key Lifetime .....	640
9	5.3.2.68	FA-HA Key SPI.....	640
10	5.3.2.69	Failure Indication .....	640
11	5.3.2.70	Target FA IP Address .....	642
12	5.3.2.71	FA Relocation Indication .....	642
13	5.3.2.72	Full DCD Setting .....	643
14	5.3.2.73	Full UCD Setting .....	643
15	5.3.2.74	Global Service Class Name .....	643
16	5.3.2.75	HA IP Address .....	643
17	5.3.2.76	HO Confirm Type .....	644
18	5.3.2.77	Home Address (HoA) .....	644
19	5.3.2.78	HO Process Optimization .....	644
20	5.3.2.79	HO Type .....	645
21	5.3.2.80	IDLE Mode Info .....	645
22	5.3.2.81	IDLE Mode Retain Info .....	645
23	5.3.2.82	IP Destination Address and Mask .....	645
24	5.3.2.83	IP Remained Time .....	646
25	5.3.2.84	IP Source Address and Mask .....	646
26	5.3.2.85	IP TOS/DSCP Range and Mask .....	646
27	5.3.2.86	Key Change Indicator .....	647
28	5.3.2.87	L-BSID .....	647
29	5.3.2.88	Location Update Status .....	647
30	5.3.2.89	AvailableInClient .....	648
31	5.3.2.90	LU Result Indicator .....	648
32	5.3.2.91	Maximum Latency .....	648
33	5.3.2.92	Maximum Sustained Traffic Rate .....	649
34	5.3.2.93	Maximum Traffic Burst .....	649
35	5.3.2.94	Media Flow Type.....	649
36	5.3.2.95	Minimum Reserved Traffic Rate .....	650
37	5.3.2.96	MIP4 Info.....	650
38	5.3.2.97	RRP .....	651
39	5.3.2.98	MN-FA Key .....	651
40	5.3.2.99	MN-FA SPI.....	651
41	5.3.2.100	MS Authorization Context .....	651
42	5.3.2.101	Target Care-of Address .....	652
43	5.3.2.102	MSID .....	653
44	5.3.2.103	MS Info .....	653
45	5.3.2.104	MS Mobility Mode .....	655
46	5.3.2.105	MS NAI .....	655
47	5.3.2.106	MS MAC Version .....	655
48	5.3.2.107	Void .....	656
49	5.3.2.108	MS Security History .....	656
50	5.3.2.109	Network Exit Indicator .....	656
51	5.3.2.110	Newer TEK Parameters .....	657
52	5.3.2.111	NRT-VR Data Delivery Service .....	657
53	5.3.2.112	Older TEK Parameters.....	658
54	5.3.2.113	Old Anchor PC ID .....	658
55	5.3.2.114	Packet Classification Rule / Media Flow Description (one or more).....	658
56	5.3.2.115	Paging Announce Timer .....	659

1	5.3.2.116	Paging Cause .....	660
2	5.3.2.117	Relay PC ID .....	660
3	5.3.2.118	Paging Cycle .....	660
4	5.3.2.119	Paging Information .....	661
5	5.3.2.120	Paging Offset .....	661
6	5.3.2.121	Paging Start/Stop .....	662
7	5.3.2.122	PC Relocation Indication .....	662
8	5.3.2.123	Paging Group ID .....	662
9	5.3.2.124	PHSF .....	662
10	5.3.2.125	PHSI .....	662
11	5.3.2.126	PHSM .....	663
12	5.3.2.127	PHS Rule .....	663
13	5.3.2.128	PHS Rule Action .....	664
14	5.3.2.129	PHSS .....	664
15	5.3.2.130	PHSV .....	664
16	5.3.2.131	PPAQ .....	665
17	5.3.2.132	Duration Used .....	666
18	5.3.2.133	PMK SN .....	666
19	5.3.2.134	PKM2 Message Code .....	666
20	5.3.2.135	Paging Interval Length .....	666
21	5.3.2.136	PN Counter .....	667
22	5.3.2.137	Preamble Index / Sub-channel Index .....	667
23	5.3.2.138	Protocol .....	667
24	5.3.2.139	Protocol Destination Port Range .....	667
25	5.3.2.140	Protocol Source Port Range .....	668
26	5.3.2.141	QoS Parameters .....	668
27	5.3.2.142	Radio Resource Fluctuation .....	669
28	5.3.2.143	Void .....	669
29	5.3.2.144	REG Context .....	669
30	5.3.2.145	Registration Type .....	670
31	5.3.2.146	Relative Delay .....	670
32	5.3.2.147	Registration Lifetime .....	671
33	5.3.2.148	Quota Identifier .....	671
34	5.3.2.149	Relocation Success Indicator .....	671
35	5.3.2.150	Request/Transmission Policy .....	672
36	5.3.2.151	Reservation Action .....	673
37	5.3.2.152	Reservation Result .....	673
38	5.3.2.153	Response Code .....	674
39	5.3.2.154	Result Code .....	674
40	5.3.2.155	Void .....	674
41	5.3.2.156	Round Trip Delay .....	674
42	5.3.2.157	RRM Absolute Threshold Value J .....	675
43	5.3.2.158	RRM Averaging Time T .....	675
44	5.3.2.159	RRM BS Info .....	676
45	5.3.2.160	RRM BS-MS PHY Quality Info .....	677
46	5.3.2.161	RRM Relative Threshold RT .....	677
47	5.3.2.162	RRM Reporting Characteristics .....	678
48	5.3.2.163	RRM Reporting Period P .....	678
49	5.3.2.164	RRM Spare Capacity Report Type .....	678
50	5.3.2.165	RT-VR Data Delivery Service .....	679
51	5.3.2.166	RxPN Counter .....	679
52	5.3.2.167	Volume Quota .....	679
53	5.3.2.168	Volume Threshold .....	679
54	5.3.2.169	SAID .....	680
55	5.3.2.170	SA Descriptor .....	680
56	5.3.2.171	Certified-MS-Feature-List-For-GW .....	680

1	5.3.2.172	SA Service Type .....	681
2	5.3.2.173	SA Type .....	681
3	5.3.2.174	SBC Context .....	681
4	5.3.2.175	SDU BSN Map .....	682
5	5.3.2.176	SDU Info .....	682
6	5.3.2.177	SDU Size .....	683
7	5.3.2.178	SDU SN .....	683
8	5.3.2.179	Service Class Name .....	683
9	5.3.2.180	Service Level Prediction .....	683
10	5.3.2.181	Service Authorization Code .....	684
11	5.3.2.182	Serving/Target Indicator .....	684
12	5.3.2.183	Certified-MS-Feature-List-For-BS .....	684
13	5.3.2.184	SFID .....	685
14	5.3.2.185	SF Info .....	685
15	5.3.2.186	Spare Capacity Indicator .....	686
16	5.3.2.187	TEK .....	686
17	5.3.2.188	TEK Lifetime .....	687
18	5.3.2.189	TEK SN .....	687
19	5.3.2.190	Tolerated Jitter .....	687
20	5.3.2.191	Total Slots DL .....	687
21	5.3.2.192	Total Slots UL .....	687
22	5.3.2.193	Traffic Priority .....	688
23	5.3.2.194	Tunnel Endpoint .....	689
24	5.3.2.195	UCD Setting .....	689
25	5.3.2.196	UGS Data Delivery Service .....	689
26	5.3.2.197	UL PHY Quality Info .....	690
27	5.3.2.198	UL PHY Service Level .....	690
28	5.3.2.199	Unsolicited Grant Interval .....	690
29	5.3.2.200	Unsolicited Polling Interval .....	690
30	5.3.2.201	VAAA IP Address .....	691
31	5.3.2.202	VAAA Realm .....	691
32	5.3.2.203	BS HO RSP Code .....	691
33	5.3.2.204	Accounting Context .....	692
34	5.3.2.205	HO ID .....	692
35	5.3.2.206	Combined Resource Indicator .....	692
36	5.3.2.207	R3 WiMAX Capability .....	693
37	5.3.2.208	R3 Accounting Capabilities .....	694
38	5.3.2.209	R3 Idle Notification Capabilities .....	694
39	5.3.2.210	R3 CUI .....	694
40	5.3.2.211	R3 Class .....	694
41	5.3.2.212	R3 Framed IP Address .....	694
42	5.3.2.213	R3 Framed-IPv6-Prefix .....	695
43	5.3.2.214	R3 WiMAX Session ID .....	695
44	5.3.2.215	R3 Packet Flow Descriptor .....	695
45	5.3.2.216	R3 Packet Data Flow ID .....	696
46	5.3.2.217	R3 Service Data Flow ID .....	696
47	5.3.2.218	R3 Service Profile ID .....	696
48	5.3.2.219	R3 Direction .....	697
49	5.3.2.220	R3 Activation Trigger .....	697
50	5.3.2.221	R3 Transport Type .....	697
51	5.3.2.222	R3 Uplink QoS ID .....	698
52	5.3.2.223	R3 Downlink QoS ID .....	698
53	5.3.2.224	R3 Uplink Classifier (This TLV is deprecated in this release) .....	698
54	5.3.2.225	R3 Downlink Classifier (This TLV is deprecated in this release) .....	698
55	5.3.2.226	R3 QoS Descriptor .....	698
56	5.3.2.227	R3 QoS ID .....	699

1	5.3.2.228	Media Flow Description in SDP Format.....	699
2	5.3.2.229	Capabilities Negotiation Mode .....	699
3	5.3.2.230	R3 Schedule Type .....	700
4	5.3.2.231	Certified-for-MCBCS .....	700
5	5.3.2.232	Certified-for-LBS.....	700
6	5.3.2.233	Certified-for-Compression.....	701
7	5.3.2.234	Certified-for-Scan-Capability .....	701
8	5.3.2.235	Certified-for-Security-Capability.....	701
9	5.3.2.236	R3 Maximum Latency .....	702
10	5.3.2.237	Reduced Resources Code.....	702
11	5.3.2.238	R3 Media Flow Type .....	702
12	5.3.2.239	Certified-for-ARQ-Capability.....	703
13	5.3.2.240	R3 SDU Size .....	703
14	5.3.2.241	R3 Unsolicited Polling Interval .....	703
15	5.3.2.242	R3 Acct Interim Interval .....	703
16	5.3.2.243	Accounting Mode Provisioning .....	704
17	5.3.2.244	Accounting Session/Flow Volume Counts .....	704
18	5.3.2.245	Accounting Number of Bulk Sessions/Flows .....	705
19	5.3.2.246	Accounting Bulk Session/Flow.....	705
20	5.3.2.247	Accounting Type.....	706
21	5.3.2.248	Interim Update Interval.....	706
22	5.3.2.249	Cumulative Uplink Octets.....	706
23	5.3.2.250	Cumulative Downlink Octets.....	706
24	5.3.2.251	Cumulative Uplink Packets.....	706
25	5.3.2.252	Cumulative Downlink Packets.....	707
26	5.3.2.253	Time of Day Tariff Switch.....	707
27	5.3.2.254	Time of Day Tariff Switch Time .....	707
28	5.3.2.255	Time of Day Tariff Switch Offset.....	707
29	5.3.2.256	Accounting Number of ToDs.....	707
30	5.3.2.257	Uplink Octets at Tariff Switch.....	708
31	5.3.2.258	Downlink Octets at Tariff Switch .....	708
32	5.3.2.259	Uplink Packets at Tariff Switch.....	708
33	5.3.2.260	Downlink Packets at Tariff Switch .....	708
34	5.3.2.261	Vendor Specific TLV.....	708
35	5.3.2.262	Paging Preference .....	709
36	5.3.2.263	Void .....	710
37	5.3.2.264	Accounting IP Address .....	710
38	5.3.2.265	Data Delivery Trigger.....	710
39	5.3.2.266	MIP4 Security Info .....	710
40	5.3.2.267	MN-FA Key Lifetime .....	711
41	5.3.2.268	Idle Mode Timeout .....	711
42	5.3.2.269	Classification Result .....	711
43	5.3.2.270	Network assisted HO Supported .....	711
44	5.3.2.271	Destination Identifier .....	712
45	5.3.2.272	Source Identifier .....	712
46	5.3.2.273	R3 Relocation Action.....	712
47	5.3.2.274	Ungraceful Network Exit Indicator.....	713
48	5.3.2.275	Duration Quota .....	713
49	5.3.2.276	Duration Threshold.....	713
50	5.3.2.277	Resource Quota.....	714
51	5.3.2.278	Resource Threshold .....	714
52	5.3.2.279	Update Reason .....	714
53	5.3.2.280	Service-ID.....	715
54	5.3.2.281	Rating-Group-ID.....	715
55	5.3.2.282	Termination Action.....	715
56	5.3.2.283	Pool-ID .....	716



1	5.3.2.284	Pool-Multiplier .....	716
2	5.3.2.285	Prepaid Server.....	716
3	5.3.2.286	R3 Active Time.....	716
4	5.3.2.287	Interim Update Interval Remaining .....	717
5	5.3.2.288	Number of UL Transport CIDs Support .....	717
6	5.3.2.289	Number of DL Transport CIDs Support .....	717
7	5.3.2.290	Classification/PHS Options and SDU Encapsulation Support.....	717
8	5.3.2.291	Maximum Number of Classifier .....	717
9	5.3.2.292	PHS Support .....	718
10	5.3.2.293	ARQ Support .....	718
11	5.3.2.294	DSx Flow Control.....	718
12	5.3.2.295	Total Number of Provisioned Service Flows .....	718
13	5.3.2.296	Maximum MAC Data per Frame Support .....	719
14	5.3.2.297	Maximum amount of MAC Level Data per DL Frame .....	719
15	5.3.2.298	Maximum amount of MAC Level Data per UL Frame .....	719
16	5.3.2.299	Packing Support.....	719
17	5.3.2.300	MAC ertPS Support .....	720
18	5.3.2.301	Maximum Number of Bursts Transmitted Concurrently to the MS .....	720
19	5.3.2.302	HO Supported .....	720
20	5.3.2.303	HO Process Optimization MS Timer .....	720
21	5.3.2.304	Mobility Features Supported.....	720
22	5.3.2.305	Sleep Mode Recovery Time.....	721
23	5.3.2.306	Void .....	721
24	5.3.2.307	ARQ Ack Type .....	721
25	5.3.2.308	MS HO Connections Parameters Proc Time.....	721
26	5.3.2.309	MS HO TEK Proc Time .....	721
27	5.3.2.310	MAC Header and Extended Sub-Header Support.....	722
28	5.3.2.311	System Resource Retain Timer.....	722
29	5.3.2.312	MS Handover Retransmission Timer.....	722
30	5.3.2.313	Handover Indication Readiness Timer.....	722
31	5.3.2.314	BS Switching Timer.....	722
32	5.3.2.315	Power Saving Class Capability .....	723
33	5.3.2.316	Subscriber Transition Gaps.....	723
34	5.3.2.317	Maximum Transmit Power .....	723
35	5.3.2.318	Capabilities for Construction and Transmission of MAC PDUs .....	723
36	5.3.2.319	PKM Flow Control .....	723
37	5.3.2.320	Maximum Number of Supported Security Associations.....	724
38	5.3.2.321	Security Negotiation Parameters.....	724
39	5.3.2.322	Void .....	724
40	5.3.2.323	MAC Mode.....	724
41	5.3.2.324	PN Window Size.....	724
42	5.3.2.325	Extended Subheader Capability .....	724
43	5.3.2.326	HO Trigger Metric Support .....	725
44	5.3.2.327	Current Transmit Power.....	725
45	5.3.2.328	OFDMA SS FFT Sizes .....	725
46	5.3.2.329	OFDMA SS demodulator .....	725
47	5.3.2.330	OFDMA SS modulator .....	725
48	5.3.2.331	The number of UL HARQ Channel .....	726
49	5.3.2.332	OFDMA SS Permutation support .....	726
50	5.3.2.333	OFDMA SS CINR Measurement Capability .....	726
51	5.3.2.334	The number of DL HARQ Channels .....	726
52	5.3.2.335	HARQ Chase Combining and CC-IR Buffer Capability .....	726
53	5.3.2.336	OFDMA SS Uplink Power Control Support.....	727
54	5.3.2.337	OFDMA SS Uplink Power Control Scheme Switching Delay .....	727
55	5.3.2.338	OFDMA MAP Capability.....	727
56	5.3.2.339	Uplink Control Channel Support .....	727

1	5.3.2.340	OFDMA MS CSIT Capability .....	727
2	5.3.2.341	Maximum Number of Burst per Frame Capability in HARQ .....	728
3	5.3.2.342	OFDMA SS demodulator for MIMO Support .....	728
4	5.3.2.343	OFDMA SS modulator for MIMO Support .....	728
5	5.3.2.344	ARQ Context .....	729
6	5.3.2.345	ARQ Enable .....	729
7	5.3.2.346	ARQ WINDOW SIZE .....	729
8	5.3.2.347	ARQ RETRY TIMEOUT-Transmitter Delay .....	729
9	5.3.2.348	ARQ RETRY TIMEOUT-Receiver Delay .....	730
10	5.3.2.349	ARQ BLOCK LIFETIME .....	730
11	5.3.2.350	ARQ SYNC LOSS TIMEOUT .....	730
12	5.3.2.351	ARQ DELIVER IN ORDER .....	730
13	5.3.2.352	ARQ RX PURGE TIMEOUT .....	730
14	5.3.2.353	ARQ BLOCK SIZE .....	731
15	5.3.2.354	RECEIVER ARQ ACK PROCESSING TIME .....	731
16	5.3.2.355	State .....	731
17	5.3.2.356	R3 Media Flow Description in SDP Format .....	731
18	5.3.2.357	VolumeUsed .....	731
19	5.3.2.358	Time Stamp .....	732
20	5.3.2.359	Accounting Bulk Session/Flow Volume Counts .....	732
21	5.3.2.360	Offline Accounting Context .....	732
22	5.3.2.361	R3 Acct Session Time .....	732
23	5.3.2.362	R3 Visited-Framed-IP-Address .....	733
24	5.3.2.363	R3 Visited-Framed-IPv6-Prefix .....	733
25	5.3.2.364	R3 Framed-Interface-Id .....	733
26	5.3.2.365	R3 Visited-Framed-Interface-Id .....	733
27	5.3.2.366	Delete MS Context Indication .....	733
28	5.3.2.367	HO Authorization Policy Support .....	734
29	5.3.2.368	NSP ID .....	734
30	5.3.2.369	Idle Mode Exit Indicator .....	734
31	5.3.2.370	Failure Indication Details .....	734
32	5.3.2.371	WiMAX message TLV position .....	735
33	5.3.2.372	FA Security Info .....	735
34	5.3.2.373	PMIP4 Context .....	736
35	5.3.2.374	DNS IP Address .....	736
36	5.3.2.375	Refresh IP Address Trigger .....	736
37	5.3.2.376	Authorized Network Services .....	737
38	5.3.2.377	Visited Authorized Network Services .....	737
39	5.3.2.378	Data Integrity Capability .....	738
40	5.3.2.379	Data Integrity Method .....	738
41	5.3.2.380	Data Integrity Applied .....	739
42	5.3.2.381	Pointer BSN .....	740
43	5.3.2.382	BSN ARQ State Bitmap .....	741
44	5.3.2.383	Switching Data Path ID .....	742
45	5.3.2.384	MAC Source Address and Mask .....	742
46	5.3.2.385	MAC Destination Address and Mask .....	742
47	5.3.2.386	ETYPE/SAP .....	742
48	5.3.2.387	User Priority Range .....	743
49	5.3.2.388	Void .....	743
50	5.3.2.389	Void .....	743
51	5.3.2.390	C-VID>S-VID Mapping .....	743
52	5.3.2.391	C-VLAN Priority Setting .....	743
53	5.3.2.392	VLAN ID Assignment .....	744
54	5.3.2.393	SVLAN ID .....	744
55	5.3.2.394	CVLAN ID .....	745
56	5.3.2.395	LocalConfigInfo .....	745

1	5.3.2.396	VLANTagProcessingRuleID .....	745
2	5.3.2.397	VLAN Tag Processing Rule .....	746
3	5.3.2.398	Uplink R3 GRE Key .....	746
4	5.3.2.399	Downlink R3 GRE Key .....	746
5	5.3.2.400	Hotlining Context .....	747
6	5.3.2.401	R3 Hotline-Profile-ID .....	747
7	5.3.2.402	R3 HTTP-Redirection-Rule .....	747
8	5.3.2.403	R3 IP-Redirection-Rule .....	748
9	5.3.2.404	R3 NAS-Filter-Rule .....	748
10	5.3.2.405	R3 Hotline-Session-Timer .....	748
11	5.3.2.406	Remaining Hotline Session Timer .....	748
12	5.3.2.407	R3 Hotline-Indication .....	748
13	5.3.2.408	R3 Hotlining Capability .....	749
14	5.3.2.409	DSCP .....	749
15	5.3.2.410	PHY Mode ID .....	750
16	5.3.2.411	Scheduling Service Supported .....	750
17	5.3.2.412	PMIP6 Info .....	750
18	5.3.2.413	LMA IPv6 Address .....	751
19	5.3.2.414	LMA IPv4 Address .....	751
20	5.3.2.415	MAG IPv6 Address .....	751
21	5.3.2.416	Home Network Prefix (HNP) .....	751
22	5.3.2.417	PMIP6 Security Indicator .....	751
23	5.3.2.418	DHCP Proxy Type .....	752
24	5.3.2.419	PMIP6 Security Info .....	752
25	5.3.2.420	MAG-LMA-PMIP6 Key .....	752
26	5.3.2.421	MAG-LMA-PMIP6 SPI .....	752
27	5.3.2.422	MAG-LMA-PMIP6-Lifetime .....	752
28	5.3.2.423	Mobility Access Classifier .....	753
29	5.3.2.424	Reattachment Zone .....	753
30	5.3.2.425	BS Location .....	753
31	5.3.2.426	WiMAX Release Info .....	753
32	5.3.2.427	R4R6R8 WiMAX Release .....	754
33	5.3.2.428	Capabilities Info .....	754
34	5.3.2.429	Support-of-MCBCS .....	755
35	5.3.2.430	Support-of-HO-DI .....	755
36	5.3.2.431	Support-of-dMAC .....	755
37	5.3.2.432	Support-of-Accounting .....	755
38	5.3.2.433	Support-of-IMS-ES .....	756
39	5.3.2.434	Support-of-PCC-QoS .....	756
40	5.3.2.435	Support-of-EtherServ .....	756
41	5.3.2.436	Support-of-LBS .....	757
42	5.3.2.437	Support-of-FixedNom .....	757
43	5.3.2.438	Support-of-Hotlining .....	757
44	5.3.2.439	Support-of-RRM .....	757
45	5.3.2.440	R6_Context_ID .....	758
46	5.3.2.441	R3 WiMAX-Release .....	758
47	5.3.2.442	Last Reset Time .....	759
48	5.3.2.443	Health Status .....	759
49	5.3.2.444	Status .....	760
50	5.3.2.445	Reported Node ID .....	760
51	5.3.2.446	Reference Last Reset Time .....	760
52	5.3.2.447	Function ID .....	760
53	5.3.2.448	ARQ Window Info .....	761
54	5.3.2.449	Starting ARQ BSN .....	761
55	5.3.2.450	Last ARQ BSN .....	761
56	5.3.2.451	Valid ARQ BSN .....	761

1	5.3.2.452	Reset Status.....	762
2	5.3.2.453	HARQ Context .....	762
3	5.3.2.454	HARQ Enable .....	762
4	5.3.2.455	HARQ Channel Mapping .....	762
5	5.3.2.456	PDU SN extended subheader for HARQ reordering .....	763
6	5.4	RADIUS Messages and Attributes .....	764
7	5.4.1	<i>RADIUS Messages</i> .....	764
8	5.4.1.1	Network Access Authentication between NAS and HAAA .....	764
9	5.4.1.2	RADIUS Messages for MIP between HA/LMA and HAAA .....	775
10	5.4.1.3	RADIUS Messages between DHCP and HAAA .....	780
11	5.4.1.4	RADIUS Message for Hot-Lining.....	781
12	5.4.1.5	Messages for Online-Accounting.....	783
13	5.4.1.6	Offline Accounting .....	784
14	5.4.1.6.1	Status and Type .....	784
15	5.4.1.6.2	Record Correlators.....	785
16	5.4.1.6.3	User Identification .....	786
17	5.4.1.6.4	Infrastructure Identifiers .....	787
18	5.4.1.6.5	Time .....	788
19	5.4.1.6.6	L3 Counters .....	788
20	5.4.1.6.7	Flow Specification.....	789
21	5.4.1.6.8	Granted-QoS.....	789
22	5.4.1.6.9	Flow Specification V2.....	790
23	5.4.1.7	RADIUS Disconnect Request Message.....	790
24	5.4.1.7.1	RADIUS Disconnect NACK Message .....	791
25	5.4.2	<i>WiMAX RADIUS VSAs Definitions</i> .....	791
26	5.4.2.1	WiMAX-Capability .....	793
27	5.4.2.2	Void .....	800
28	5.4.2.3	GMT-Time-Zone-Offset.....	800
29	5.4.2.4	WiMAX-Session-Id .....	800
30	5.4.2.5	MSK.....	801
31	5.4.2.6	hHA-IP-MIP4 .....	801
32	5.4.2.7	hHA-IP-MIP6 .....	801
33	5.4.2.8	hDHCPv4-Server.....	802
34	5.4.2.9	hDHCPv6-Server.....	802
35	5.4.2.10	MN-hHA-MIP4-KEY .....	803
36	5.4.2.11	MN-hHA-MIP4-SPI .....	803
37	5.4.2.12	MN-hHA-MIP6-KEY .....	804
38	5.4.2.13	MN-hHA-MIP6-SPI .....	804
39	5.4.2.14	FA-RK-KEY .....	805
40	5.4.2.15	hHA-RK-KEY .....	805
41	5.4.2.16	hHA-RK-SPI.....	806
42	5.4.2.17	hHA-RK-Lifetime.....	806
43	5.4.2.18	RRQ-HA-IP .....	806
44	5.4.2.19	RRQ-MN-HA-KEY .....	807
45	5.4.2.20	Time-Of-Day-Time.....	807
46	5.4.2.21	Session-Continue .....	808
47	5.4.2.22	Beginning-of-Session.....	809
48	5.4.2.23	Network-Technology .....	809
49	5.4.2.24	Hotline-Indication.....	810
50	5.4.2.25	Prepaid-Indicator .....	810
51	5.4.2.26	PDFID.....	811
52	5.4.2.27	SDFID.....	811
53	5.4.2.28	Packet-Flow Descriptor (This Attribute is deprecated in this release).....	811
54	5.4.2.29	QoS-Descriptor .....	812
55	5.4.2.30	Uplink-Granted-QoS.....	818
56	5.4.2.31	Control-Packets-In.....	818

1	5.4.2.32	Control-Octets-In .....	819
2	5.4.2.33	Control-Packets-Out .....	819
3	5.4.2.34	Control-Octets-Out .....	820
4	5.4.2.35	PPAC .....	820
5	5.4.2.36	Session Termination Capability .....	821
6	5.4.2.37	PPAQ Attribute .....	821
7	5.4.2.38	Prepaid Tariff Switching Attribute (PTS) .....	828
8	5.4.2.39	Active-Time .....	830
9	5.4.2.40	hDHCP-RK .....	830
10	5.4.2.41	hDHCP-RK-Key-ID .....	831
11	5.4.2.42	hDHCP-RK-Lifetime .....	831
12	5.4.2.43	DHCPMSG-Server-IP .....	831
13	5.4.2.44	Idle-Mode-Transition .....	832
14	5.4.2.45	NAP-ID .....	832
15	5.4.2.46	BS-ID .....	833
16	5.4.2.47	Location .....	833
17	5.4.2.48	Acct- Input -Packets-Gigaword .....	833
18	5.4.2.49	Acct- Output -Packets Gigaword .....	834
19	5.4.2.50	Uplink Flow Description .....	834
20	5.4.2.51	BU-CoA-Ipv6 .....	835
21	5.4.2.52	DNS .....	835
22	5.4.2.53	Hotline-Profile-ID .....	836
23	5.4.2.54	HTTP-Redirection-Rule .....	836
24	5.4.2.55	IP-Redirection-Rule .....	837
25	5.4.2.56	Hotline-Session-Timer .....	838
26	5.4.2.57	NSP-ID .....	838
27	5.4.2.58	Void .....	839
28	5.4.2.59	Count-Type .....	839
29	5.4.2.60	WiMAX-DM-Action-Code .....	839
30	5.4.2.61	FA-RK-SPI .....	840
31	5.4.2.62	Downlink Flow Description .....	840
32	5.4.2.63	Downlink-Granted-QoS .....	841
33	5.4.2.64	vHA-IP-MIP4 .....	841
34	5.4.2.65	vHA-IP-MIP6 .....	841
35	5.4.2.66	MN-vHA-MIP4-KEY .....	842
36	5.4.2.67	vHA-RK-KEY .....	842
37	5.4.2.68	vHA-RK-SPI .....	843
38	5.4.2.69	vHA-RK-Lifetime .....	843
39	5.4.2.70	MN-vHA-MIP4-SPI .....	843
40	5.4.2.71	vDHCPv4-Server .....	844
41	5.4.2.72	vDHCPv6-Server .....	844
42	5.4.2.73	vDHCP-RK .....	845
43	5.4.2.74	vDHCP-RK-Key-ID .....	845
44	5.4.2.75	vDHCP-RK-Lifetime .....	846
45	5.4.2.76	PMIP-Authenticated-Network-Identity .....	846
46	5.4.2.77	Visited-Framed-IP-Address .....	846
47	5.4.2.78	Visited-Framed-IPv6-Prefix .....	847
48	5.4.2.79	Visited-Framed-Interface-Id .....	847
49	5.4.2.80	MIP-Authorization-Status .....	847
50	5.4.2.81	Flow-Description-V2 .....	848
51	5.4.2.82	Packet-Flow-Descriptor-V2 .....	848
52	5.4.2.83	Classifier .....	852
53	5.4.2.84	Source/Destination Specification .....	855
54	5.4.2.85	ETH Option .....	858
55	5.4.2.86	ETH Proto Type .....	859
56	5.4.2.87	ETH VLAN ID .....	859

1	5.4.2.88	ETH Priority Range .....	860
2	5.4.2.89	VLANTagProcessing Descriptor .....	861
3	5.4.2.90	hDHCP-Server-Parameters .....	864
4	5.4.2.91	vDHCP-Server-Parameters .....	865
5	5.4.2.92	PMIP6-Service-Info .....	867
6	5.4.2.93	hLMA-IPv6-PMIP6 .....	867
7	5.4.2.94	hLMA-IPv4-PMIP6 .....	868
8	5.4.2.95	vLMA-IPv6-PMIP6 .....	868
9	5.4.2.96	vLMA-IPv4-PMIP6 .....	868
10	5.4.2.97	PMIP6-RK-KEY .....	869
11	5.4.2.98	PMIP6-RK-SPI .....	869
12	5.4.2.99	Home-HNP-PMIP6 .....	870
13	5.4.2.100	Home-Interface-Id-PMIP6 .....	870
14	5.4.2.101	Home-IPv4-HoA-PMIP6 .....	870
15	5.4.2.102	Visited-HNP-PMIP6 .....	871
16	5.4.2.103	Visited-Interface-Id-PMIP6 .....	871
17	5.4.2.104	Visited-IPv4-HoA-PMIP6 .....	872
18	5.4.2.105	BS-Location .....	872
19	5.4.2.106	Mobility-Access-Classfier .....	872
20	5.4.2.107	MS-Authenticated .....	873
21	5.4.2.108	Operator-Name .....	873
22	5.4.2.109	Certified-MS-Feature-List-For-GW .....	874
23	5.4.2.110	Certified-MS-Feature-List-For-BS .....	875
24	5.5	Diameter Applications, Commands and AVPs .....	877
25	5.5.1	<i>Diameter Applications and Messages</i> .....	878
26	5.5.1.1	WiMAX Network Access Authentication and Authorization Diameter Application .....	878
27	5.5.1.1.1	WiMAX Diameter-EAP-Request/Answer Commands .....	878
28	5.5.1.1.2	WiMAX Change-of-Authorization-Request/Answer Command .....	895
29	5.5.1.1.3	WiMAX Reauthentication Request/Answer Command .....	897
30	5.5.1.1.4	WiMAX Session Termination Request/Answer Command .....	902
31	5.5.1.1.5	WiMAX Abort Session Request/Answer Command .....	905
32	5.5.1.2	WiMAX MIP4 Diameter Application .....	909
33	5.5.1.2.1	WiMAX-Home-Agent-IPv4-Request /Answer Command .....	910
34	5.5.1.3	WiMAX MIP6 Diameter Application .....	915
35	5.5.1.3.1	WiMAX MIP6 Request/Answer Commands .....	916
36	5.5.1.4	WiMAX DHCP Diameter Application .....	920
37	5.5.1.4.1	WiMAX DHCP Request/Answer Commands .....	920
38	5.5.1.5	Messages for Online-Accounting .....	923
39	5.5.1.5.1	Initialization, maintenance and termination of connection and session .....	923
40	5.5.1.5.2	R3-OC Auth-Application-ID .....	923
41	5.5.1.5.3	Credit-Control-Request message .....	923
42	5.5.1.5.4	Credit-Control-Answer message .....	929
43	5.5.1.5.5	R3-OC specific AVPs .....	934
44	5.5.1.5.6	R3-OC Re-Used AVPs of external organizations .....	935
45	5.5.1.5.7	Mobility handling .....	938
46	5.5.1.6	Offline Accounting .....	938
47	5.5.1.6.1	Accounting-Request Message .....	938
48	5.5.1.6.2	Accounting-Answer Message .....	941
49	5.5.1.6.3	Overview of Diameter AVPs used for PCC-R3-OFC Reference points .....	942
50	5.5.1.6.4	AVP Occurrence Table .....	945
51	5.5.2	<i>WiMAX DIAMETER VSAs Definitions</i> .....	950
52	5.5.2.1	WiMAX-Capability .....	950
53	5.5.2.2	Device-Authentication-Indicator .....	951
54	5.5.2.3	GMT-Time-Zone-Offset .....	951
55	5.5.2.4	WiMAX-Session-Id .....	952
56	5.5.2.5	MSK .....	952

1	5.5.2.6	hHA-IP-MIP4 .....	952
2	5.5.2.7	hHA-IP-MIP6 .....	952
3	5.5.2.8	hDHCPv4-Server .....	952
4	5.5.2.9	hDHCPv6-Server .....	953
5	5.5.2.10	MN-HA-MIP4-KEY .....	953
6	5.5.2.11	MN-HA-MIP4-SPI .....	953
7	5.5.2.12	MN-HA-MIP6-KEY .....	953
8	5.5.2.13	MN-HA-MIP6-SPI .....	953
9	5.5.2.14	FA-RK-KEY .....	953
10	5.5.2.15	HA-RK-KEY .....	953
11	5.5.2.16	HA-RK-SPI.....	953
12	5.5.2.17	HA-RK-Lifetime.....	954
13	5.5.2.18	RRQ-HA-IP .....	954
14	5.5.2.19	RRQ-MN-HA-KEY .....	954
15	5.5.2.20	Session-Continue .....	954
16	5.5.2.21	Beginning-of-Session.....	954
17	5.5.2.22	Network-Technology .....	955
18	5.5.2.23	Hotline-Indication.....	955
19	5.5.2.24	Prepaid-Indicator .....	955
20	5.5.2.25	PDFID.....	955
21	5.5.2.26	SDFID.....	956
22	5.5.2.27	Packet-Flow-Descriptor (This AVP is deprecated in this release).....	956
23	5.5.2.28	QoS-Descriptor .....	956
24	5.5.2.29	Control-Packets-In .....	958
25	5.5.2.30	Control-Octets-In .....	958
26	5.5.2.31	Control-Packets-Out .....	959
27	5.5.2.32	Control-Octets-Out .....	959
28	5.5.2.33	Active-Time .....	959
29	5.5.2.34	DHCP-RK.....	959
30	5.5.2.35	DHCP-RK-Key-ID .....	959
31	5.5.2.36	DHCP-RK-Lifetime.....	959
32	5.5.2.37	DHCPMSG-Server-IP .....	960
33	5.5.2.38	Idle-Mode-Transition.....	960
34	5.5.2.39	NAP-ID .....	960
35	5.5.2.40	BS-ID .....	960
36	5.5.2.41	Location .....	960
37	5.5.2.42	Acct-Input-Packets-Gigaword .....	961
38	5.5.2.43	Acct-Output-Packets Gigaword .....	961
39	5.5.2.44	Flow-Description .....	961
40	5.5.2.45	BU-CoA-Ipv6 .....	961
41	5.5.2.46	DNS .....	961
42	5.5.2.47	Hotline-Profile-ID.....	961
43	5.5.2.48	HTTP-Redirection-Rule.....	961
44	5.5.2.49	IP-Redirection-Rule .....	962
45	5.5.2.50	Hotline-Session-Timer.....	963
46	5.5.2.51	NSP-ID .....	963
47	5.5.2.52	HA-RK-Key-Requested.....	964
48	5.5.2.53	Count-Type .....	964
49	5.5.2.54	FA-RK-SPI .....	964
50	5.5.2.55	vHA-IP-MIP4 .....	964
51	5.5.2.56	vHA-IP-MIP6 .....	964
52	5.5.2.57	vDHCPv4-Server .....	964
53	5.5.2.58	vDHCPv6-Server .....	964
54	5.5.2.59	PMIP-Authenticated-Network-Identity .....	965
55	5.5.2.60	Visited-Framed-IP-Address .....	965
56	5.5.2.61	Visited-Framed-IPv6-Address .....	965

1	5.5.2.62	Visited-Framed-Interface-Id .....	965
2	5.5.2.63	Packet-Flow-Descriptor-V2 .....	965
3	5.5.2.64	VLANTagProcessing-Descriptor .....	967
4	5.5.2.65	WiMAX-Release .....	968
5	5.5.2.66	Accounting-Capabilities .....	968
6	5.5.2.67	Hotlining-Capabilities .....	969
7	5.5.2.68	Idle-Mode-Notification-Capabilities .....	969
8	5.5.2.69	ServiceProfileID .....	969
9	5.5.2.70	Direction .....	969
10	5.5.2.71	Activation-Trigger .....	970
11	5.5.2.72	Transport-Type .....	970
12	5.5.2.73	UplinkQoSID .....	970
13	5.5.2.74	DownlinkQoSID .....	971
14	5.5.2.75	IP-Classifer .....	971
15	5.5.2.76	QoS-ID .....	971
16	5.5.2.77	Global-Service-Class-Name .....	971
17	5.5.2.78	Service-Class-Name .....	972
18	5.5.2.79	Schedule-Type .....	972
19	5.5.2.80	Traffic-Priority .....	972
20	5.5.2.81	Maximum-Sustained-Traffic-Rate .....	973
21	5.5.2.82	Minimum-Reserved-Traffic-Rate .....	973
22	5.5.2.83	Maximum-Traffic-Burst .....	973
23	5.5.2.84	Tolerated-Jitter .....	973
24	5.5.2.85	Maximum-Latency .....	973
25	5.5.2.86	Reduced-Resources-Code .....	974
26	5.5.2.87	Media-Flow-Type .....	974
27	5.5.2.88	Unsolicited-Grant-Interval .....	974
28	5.5.2.89	SDU-Size .....	975
29	5.5.2.90	Unsolicited-Polling-Interval .....	975
30	5.5.2.91	MN-HA-MIP4-MSA .....	975
31	5.5.2.92	MN-vHA-MIP4-MSA .....	976
32	5.5.2.93	FA-RK-MSA .....	976
33	5.5.2.94	HA-RK-MSA .....	977
34	5.5.2.95	vHA-RK-MSA .....	977
35	5.5.2.96	DHCP-RK-SA .....	978
36	5.5.2.97	vDHCP-RK-SA .....	978
37	5.5.2.98	Redirect-Action .....	979
38	5.5.2.99	Redirect-URL .....	979
39	5.5.2.100	SA-SPI .....	979
40	5.5.2.101	SA-KEY .....	979
41	5.5.2.102	SA-Lifetime .....	980
42	5.5.2.103	Redirect-Address .....	980
43	5.5.2.104	Redirect-Port .....	980
44	5.5.2.105	DHCPv6-RK-SA .....	980
45	5.5.2.106	vDHCPv6-RK-SA .....	981
46	5.5.2.107	Packet-Flow-Descriptor-Capabilities (This TLV is deprecated in this release) .....	981
47	5.5.2.108	Authorized-Network-Services .....	981
48	5.5.2.109	ASN-Network-Service-Capabilities .....	982
49	5.5.2.110	VCSN-Network-Service-Capabilities .....	982
50	5.5.2.111	Visited-Authorized-Network-Services .....	983
51	5.5.2.112	Paging-Preference .....	983
52	5.5.2.113	VLANTagProcessingRuleID .....	983
53	5.5.2.114	Media-Flow-Description-In-SDP-Format .....	983
54	5.5.2.115	Transmission-Policy .....	984
55	5.5.2.116	Classifier .....	984
56	5.5.2.117	Classifier-ID .....	985



1	5.5.2.118	Priority .....	985
2	5.5.2.119	Direction .....	985
3	5.5.2.120	Action .....	986
4	5.5.2.121	Protocol .....	986
5	5.5.2.122	From-Spec .....	986
6	5.5.2.123	To-Spec .....	988
7	5.5.2.124	IP-TOS/DSCP-Range-And-Mask .....	990
8	5.5.2.125	ETH-Option .....	990
9	5.5.2.126	ETH-Proto-Type .....	990
10	5.5.2.127	VLAN-ID-Range .....	991
11	5.5.2.128	ETH-Priority-Range .....	991
12	5.5.2.129	ETH-Ether-Type .....	991
13	5.5.2.130	ETH-SAP .....	992
14	5.5.2.131	S-VID-Start .....	992
15	5.5.2.132	S-VID-End .....	992
16	5.5.2.133	C-VID-Start .....	992
17	5.5.2.134	C-VID-End .....	992
18	5.5.2.135	ETH-Low-Priority .....	992
19	5.5.2.136	ETH-High-Priority .....	992
20	5.5.2.137	IP-Address .....	992
21	5.5.2.138	IP-Address-Range .....	993
22	5.5.2.139	IP-Address-Mask .....	993
23	5.5.2.140	Port .....	993
24	5.5.2.141	Port-Range .....	993
25	5.5.2.142	Negated .....	994
26	5.5.2.143	User-Assigned-Address .....	994
27	5.5.2.144	MAC-Address .....	994
28	5.5.2.145	MAC-Mask .....	994
29	5.5.2.146	IP-Address-Start .....	994
30	5.5.2.147	IP-Address-End .....	995
31	5.5.2.148	IP-Bit-Mask-Width .....	995
32	5.5.2.149	Port-Start .....	995
33	5.5.2.150	Port-End .....	995
34	5.5.2.151	MAC-Address-Mask-Pattern .....	995
35	5.5.2.152	C-VLAN-Priority-Setting .....	995
36	5.5.2.153	VLAN-ID-Assignment .....	995
37	5.5.2.154	C-VLAN-ID .....	996
38	5.5.2.155	S-VLAN-ID .....	996
39	5.5.2.156	C-VID-To-S-VID-Mapping .....	996
40	5.5.2.157	Local-Config-Info .....	996
41	5.5.2.158	hDHCP-Server-Parameters .....	997
42	5.5.2.159	vDHCP-Server-Parameters .....	997
43	5.5.2.160	DSCP .....	998
44	5.5.2.161	BS-Location .....	998
45	5.5.2.162	Mobility-Access-Classifer .....	998
46	5.5.2.163	Mobility-Access-Capabilities .....	998
47	5.5.2.164	ROHC-Support .....	999
48	5.5.2.165	R3-OC-Session-Continue .....	999
49	5.5.2.166	Old-Session-Id .....	999
50	5.5.2.167	WiMAX-Information .....	999
51	5.5.2.168	Uplink-Granted-QoS .....	1001
52	5.5.2.169	Downlink-Granted-QoS .....	1002
53	5.5.2.170	Interim-Cause .....	1003
54	5.5.2.171	MS-Authenticated .....	1003
55	5.5.2.172	Release-Supported .....	1003
56	5.5.2.173	Version-Negotiation-Flag .....	1003

1	5.5.2.174	Certified-MS-Feature-List-For-GW .....	1004
2	5.5.2.175	Certified-MS-Feature-List-For-BS .....	1004
3	5.5.2.176	Certified-For-MCBCS .....	1005
4	5.5.2.177	Certified-For-LBS.....	1005
5	5.5.2.178	Certified-Compression.....	1006
6	5.5.2.179	Certified-Scan-Capability .....	1006
7	5.5.2.180	Certified-Security-Capability.....	1006
8	5.5.2.181	Certified-ARQ-Capability.....	1007
9	5.5.3	<i>Reused Diameter AVPs .....</i>	<i>1007</i>
10	5.5.3.1	Session-Id .....	1007
11	5.5.3.2	Acct-Session-Id.....	1007
12	5.5.3.3	Acct-Multi-Session-Id .....	1008
13	5.5.3.4	Acct-Application-Id .....	1008
14	5.5.3.5	NAS-IP-Address .....	1008
15	5.5.3.6	NAS-IPv6-Address .....	1008
16	5.5.3.7	Service-Context-Id.....	1008
17	5.5.3.8	Multiple-Services-Credit-Control .....	1009
18	5.5.3.9	Access-Network-Charging-Identifier-Gx .....	1010
19	5.5.3.10	Service-Information .....	1010
20	5.5.3.11	Operator-Name .....	1011
21	5.6	DHCP Vendor Specific Options .....	1012
22	5.6.1	<i>WiMAX Radio Link Characteristics vendor specific option .....</i>	<i>1012</i>
23	5.7	IP Mobility Messages .....	1014
24	5.7.1	<i>PMIP6 Messages.....</i>	<i>1014</i>
25	5.7.1.1	PBU and PBA messages .....	1014
26	5.7.1.2	BRI and BRA messages.....	1016
27	5.8	TLV Definitions for EAP-Notification.....	1017
28	5.8.1	<i>Notification-Information .....</i>	<i>1017</i>
29	5.8.2	<i>Notification-Code .....</i>	<i>1017</i>
30	5.8.3	<i>Network Rejection Information .....</i>	<i>1017</i>
31	5.8.4	<i>Rejection Code .....</i>	<i>1018</i>
32	5.8.5	<i>Allowed Location Information.....</i>	<i>1020</i>
33	5.8.6	<i>Received NAI .....</i>	<i>1020</i>
34	5.8.7	<i>Emergency Services Override .....</i>	<i>1020</i>
35	5.8.8	<i>RMAC (Rejection Message Authentication Code) Value .....</i>	<i>1021</i>
36	6.	DATA PLANE.....	1022
37	6.1	Encapsulation on R3 .....	1022
38	6.1.1	<i>IP in IP Encapsulation .....</i>	<i>1022</i>
39	6.1.2	<i>GRE Encapsulation .....</i>	<i>1022</i>
40	6.1.3	<i>Other Encapsulation.....</i>	<i>1023</i>
41	6.2	GRE Encapsulation on R4 and R6.....	1023
42	6.3	Convergence Sublayer on R1 .....	1024
43	6.3.1	<i>IP-CS.....</i>	<i>1024</i>
44	6.3.2	<i>IPoETH-CS.....</i>	<i>1024</i>
45	6.3.3	<i>ETH-CS .....</i>	<i>1025</i>
46	7.	FEATURE LIST FOR NWG REL 1.5.....	1026
47			
48			
49			

## List of Figures

FIGURE 3-1 – BIT ORDERING .....	6
FIGURE 3-2 – MESSAGE FORMAT .....	7
FIGURE 3-3 – FLAGS FORMAT .....	7
FIGURE 3-4 – EXAMPLE OF ASN SEPARATED INTO TWO PRIVATE IP CLOUDS .....	10
FIGURE 3-5 – COMMUNICATION MODEL .....	11
FIGURE 3-6 – PROTOCOL LAYERS .....	12
FIGURE 4-1 – BASE STATION ID FORMAT FOR NETWORK DISCOVERY AND SELECTION .....	21
FIGURE 4-2 – NETWORK DISCOVERY AND SELECTION SDL .....	28
FIGURE 4-3 – WIMAX KEY HIERARCHY .....	33
FIGURE 4-4 – SPI COLLISION AVOIDANCE MECHANISM .....	36
FIGURE 4-5 – KEY DISTRIBUTION .....	37
FIGURE 4-6 – REPLAY PROTECTION FOR REENTRY, HANDOVER, AND SECURE LOCATION UPDATE .....	42
FIGURE 4-7 – CMIP4 KEY DISTRIBUTION WITHOUT FA RELOCATION .....	46
FIGURE 4-8 – CMIP4 KEY DISTRIBUTION WITH FA RELOCATION .....	48
FIGURE 4-9 – PMIP4 KEY DISTRIBUTION .....	49
FIGURE 4-10 – PMIP6 KEY DISTRIBUTION .....	50
FIGURE 4-11 – INITIAL DHCP KEY DISTRIBUTION .....	52
FIGURE 4-12 – DHCP KEY DISTRIBUTION WHEN AUTHENTICATOR AND DHCP RELAY ARE NOT COLLOCATED .....	54
FIGURE 4-13 – REAUTHENTICATION PROCEDURE (W/O AUTHENTICATOR RELOCATION) .....	74
FIGURE 4-14 – AUTHENTICATOR RELOCATION PROCEDURE (PULL) .....	82
FIGURE 4-15 – AUTHENTICATOR RELOCATION (PUSH) .....	92
FIGURE 4-16 – AUTHENTICATOR UPDATE NOTIFICATION PROCEDURE .....	96
FIGURE 4-17 – ACCOUNTING MODES AND TERMINOLOGY .....	104
FIGURE 4-18 – ONLINE ACCOUNTING PROCEDURES .....	106
FIGURE 4-19 – INITIAL AND PRE-PROVISIONED SERVICE FLOW CREATION .....	108
FIGURE 4-20 –SESSION TERMINATION .....	109
FIGURE 4-21 – PPC RELOCATION .....	111
FIGURE 4-22 – PPC RELOCATION PROCEDURE .....	113
FIGURE 4-23 – PPA RELOCATION .....	116
FIGURE 4-24 – PPA-PPC QUOTA(S) UPDATE .....	118
FIGURE 4-25 – ACCOUNTING CLIENT AND AGENT .....	121
FIGURE 4-26 – OFFLINE ACCOUNTING PROCEDURES .....	122
FIGURE 4-27 – CORRELATION HIERARCHY .....	125
FIGURE 4-28 – BULK INTERIM UPDATE PROCEDURE .....	127
FIGURE 4-29 – HOT-LINING .....	128
FIGURE 4-30 – IDLE MODE ENTRY .....	129
FIGURE 4-31 – IDLE MODE EXIT .....	129
FIGURE 4-32 – NETWORK EXIT .....	130
FIGURE 4-33 – ACCOUNTING CLIENT RELOCATION .....	131
FIGURE 4-34 – ACTIVE IP SESSION HOT-LINING .....	134
FIGURE 4-35 – ACTIVE IP SESSION HOT-LINING FOR PREPAID USER ACCOUNT REPLENISHMENT .....	137
FIGURE 4-36 – NEW IP SESSION HOT-LINING .....	138
FIGURE 4-37 – HOT-LINING DURING INITIAL NETWORK ENTRY .....	140
FIGURE 4-38 – ACCOUNTING AGENT RELOCATION .....	142
FIGURE 4-39 – CONTEXT UPDATE PROCEDURE .....	143
FIGURE 4-40 – BULK INTERIM UPDATE .....	146
FIGURE 4-41 – ACCOUNTING START EVENT IN THE ASN IN CASE OF CMIP4 .....	156
FIGURE 4-42 – ACCOUNTING START EVENT IN THE ASN IN CASE OF PMIP4 .....	157
FIGURE 4-43 – ACCOUNTING START EVENT IN THE ASN IN CASE OF SIMPLE IPV4 .....	158
FIGURE 4-44 – ACCOUNTING START EVENT IN THE ASN IN CASE OF SIMPLE IPV6 .....	159
FIGURE 4-45 – ACCOUNTING START EVENT IN THE ASN IN CASE OF CMIP6 (NOTE CMIP6 HAS NO ACCOUNTING EVENT IN ASN) .....	160

1	FIGURE 4-46 – ACCOUNTING START EVENT IN THE ASN IN CASE OF PMIP6 .....	161
2	FIGURE 4-47 – ACCOUNTING START EVENT IN THE CSN IN CASE OF CMIP4 .....	162
3	FIGURE 4-48 – ACCOUNTING START EVENT IN THE CSN IN CASE OF PMIP4 .....	163
4	FIGURE 4-49 – ACCOUNTING START EVENT IN THE CSN IN CASE OF CMIP6 .....	164
5	FIGURE 4-50 – ACCOUNTING START EVENT IN THE CSN IN CASE OF PMIP6 .....	165
6	FIGURE 4-51 – MS INITIAL NETWORK ENTRY (SINGLE EAP) .....	166
7	FIGURE 4-52 – NETWORK REJECTION PROCEDURE DURING EAP .....	181
8	FIGURE 4-53 – NETWORK REJECTION PROCEDURE FOR EAP-TLS .....	182
9	FIGURE 4-54 – NETWORK REJECTION PROCEDURE FOR EAP-TTLS .....	183
10	FIGURE 4-55 – NETWORK REJECTION PROCEDURE FOR EAP-AKA .....	184
11	FIGURE 4-56 – NETWORK REJECTION PROCEDURE IN CASE OF EAP-TTLS PHASE 2 FAILURE .....	185
12	FIGURE 4-57 – MS TRIGGERED NETWORK EXIT (NORMAL MODE) .....	189
13	FIGURE 4-58 – AAA SERVER/ AUTHENTICATOR TRIGGER (NORMAL MODE) .....	191
14	FIGURE 4-59 – ANCHOR DPF/FA TRIGGER (NORMAL MODE) .....	194
15	FIGURE 4-60 – BS TRIGGER (NORMAL MODE) .....	195
16	FIGURE 4-61 – ASN ENTITY INSTIGATING NET EXIT IN A BS .....	197
17	FIGURE 4-62 – HA INITIATED MS NETWORK EXIT .....	198
18	FIGURE 4-63 – MS TRIGGERED NETWORK EXIT (IDLE MODE) .....	199
19	FIGURE 4-64 – AAA SERVER/ AUTHENTICATOR TRIGGER UNGRACEFUL NETWORK EXIT (IDLE	
20	MODE) .....	201
21	FIGURE 4-65 – ANCHOR PC TRIGGERED UNGRACEFUL NETWORK EXIT (IDLE MODE) .....	202
22	FIGURE 4-66 – ANCHOR DPF/FA TRIGGERED UNGRACEFUL NETWORK EXIT (IDLE MODE) .....	203
23	FIGURE 4-67 – ISF CLASSIFIER UPDATE FOR IPV6 .....	211
24	FIGURE 4-68 – ISF CLASSIFIER UPDATE FOR PMIP4 .....	212
25	FIGURE 4-69 – ISF CLASSIFIER UPDATE FOR CMIP4 .....	213
26	FIGURE 4-70 – ISF CLASSIFIER UPDATE FOR PMIP6 .....	214
27	FIGURE 4-71 – AAA-TRIGGERED QOS PROFILE UPDATE .....	217
28	FIGURE 4-72 – SFA-TRIGGERED SERVICE FLOW CREATION (PROFILE DOWNLOADED IN SFA) .....	218
29	FIGURE 4-73 – MS INITIATED SERVICE FLOW CREATION .....	220
30	FIGURE 4-74 – MS INITIATED SERVICE FLOW MODIFICATION .....	222
31	FIGURE 4-75 – SFA-TRIGGERED SERVICE FLOW DELETION .....	224
32	FIGURE 4-76 – MS-TRIGGERED SERVICE FLOW DELETION .....	225
33	FIGURE 4-77 – SUCCESSFUL HO PREPARATION PHASE, SCENARIO 1 .....	266
34	FIGURE 4-78 – SUCCESSFUL HO PREPARATION PHASE, SCENARIO 2 .....	268
35	FIGURE 4-79 – SUCCESSFUL HO PREPARATION PHASE, SCENARIO 3 .....	270
36	FIGURE 4-80 – SUCCESSFUL HO PREPARATION PHASE, SCENARIO 5 .....	271
37	FIGURE 4-81 – SUCCESSFUL HO PREPARATION PHASE (THE SERVING, RELAY AND THE	
38	AUTHENTICATOR ASN-GW ARE COLLOCATED) .....	273
39	FIGURE 4-82 – SUCCESSFUL HO PREPARATION PHASE (NETWORK INITIATED) .....	275
40	FIGURE 4-83 – SUCCESSFUL HO ACTION PHASE, SCENARIO 1 .....	281
41	FIGURE 4-84 – SUCCESSFUL HO ACTION PHASE, SCENARIO 2 .....	284
42	FIGURE 4-85 – SUCCESSFUL HO ACTION PHASE, SCENARIO 3 .....	286
43	FIGURE 4-86 – SUCCESSFUL HO ACTION PHASE, SCENARIO 4 .....	289
44	FIGURE 4-87 – R4 HO CANCELLATION, SCENARIO 1 .....	292
45	FIGURE 4-88 – R4 HO CANCELLATION, SCENARIO 2 .....	293
46	FIGURE 4-89 – HO CANCELLATION, SCENARIO 3 .....	294
47	FIGURE 4-90 – HO CANCELLATION, SCENARIO 4 .....	295
48	FIGURE 4-91 – MS HANDOVER REJECTION .....	296
49	FIGURE 4-92 – UNCONTROLLED (UNPREDICTIVE) HO .....	300
50	FIGURE 4-93 – HO AND SCANNING CONTROL FOR FIXED/NOMADIC SS/MS .....	302
51	FIGURE 4-94 – SUCCESSFUL MS INITIATED HO PREPARATION .....	340
52	FIGURE 4-95 – SUCCESSFUL NETWORK INITIATED HO PREPARATION PHASE .....	341
53	FIGURE 4-96 – MAC CONTEXT RETRIEVAL PROCEDURE .....	344
54	FIGURE 4-97 – SUCCESSFUL HO ACTION PHASE, SCENARIO 1 .....	345
55	FIGURE 4-98 – SUCCESSFUL HO ACTION PHASE, SCENARIO 2 .....	347
56	FIGURE 4-99 – SUCCESSFUL HO ACTION PHASE, SCENARIO 3 .....	348

1	FIGURE 4-100 – PATH DE-REGISTRATION WITH OLD SERVING AND UNSELECTED TARGET BSS	350
2	FIGURE 4-101 –HO CANCELLATION, SCENARIO 1	351
3	FIGURE 4-102 –HO CANCELLATION, SCENARIO 3	352
4	FIGURE 4-103 – HO REJECT	353
5	FIGURE 4-104 – UNCONTROLLED (UNPREDICTIVE) HO	355
6	FIGURE 4-105 – PER SF DATA PATH TREE AFTER HO PREPARATION PHASE	357
7	FIGURE 4-106 – TRANSMISSION QUEUES IN SERVING BS AND TARGET BS	358
8	FIGURE 4-107 – EXAMPLE OF TRANSMISSION QUEUE IN THE SERVING BS	359
9	FIGURE 4-108 – DATA BUFFERING AND FORWARDING IN BS BUFFER SWITCHING	361
10	FIGURE 4-109 – DATA DELIVERY VIA ANCHOR ASN-GW	363
11	FIGURE 4-110 – DATA BUFFERING AT THE SERVING BS AND FORWARDING VIA R8	366
12	FIGURE 4-111 – DATA INTEGRITY PROCEDURES FOR DIRECT DATA DELIVERY METHOD	367
13	FIGURE 4-112 – EXAMPLE OF PER-SF DOWNLINK TRANSMISSION QUEUE IN SERVING BS	374
14	FIGURE 4-113 – EXAMPLE OF PER-SF UPLINK RECEPTION QUEUE IN SERVING BS	376
15	FIGURE 4-114 – DATA INTEGRITY PACKETS TO FORWARD ARQ BLOCKS (EXAMPLE)	377
16	FIGURE 4-115 – RECONSTRUCTION OF ARQ BUFFERS AND STATE MACHINES AT TARGET BS	
17	(EXAMPLE)	378
18	FIGURE 4-116 – FIELDS OF THE OUTER HEADER RELEVANT FOR UPLINK SDU REASSEMBLY AT	
19	ANCHOR ASN-GW	380
20	FIGURE 4-117 – UPLINK DATA PATH TREE	380
21	FIGURE 4-118 – FIRST FRAGMENT SENT FROM THE SBS	382
22	FIGURE 4-119 – SECOND FRAGMENT SENT FROM THE SBS	382
23	FIGURE 4-120 – FRAGMENT SENT FROM THE TBS	383
24	FIGURE 4-121 – DATA INTEGRITY PACKETS TO FORWARD ARQ BLOCKS (EXAMPLE)	384
25	FIGURE 4-122 – PMIP4 CONNECTION SETUP PROCEDURE	398
26	FIGURE 4-123– DHCP SESSION RENEWAL IN PMIP4 CASE VIA DHCP REQUEST - DHCP PROXY IN ASN	
27		400
28	FIGURE 4-124 – PMIP4 CONNECTION SETUP - DHCP RELAY IN ASN	401
29	FIGURE 4-125 - DHCP SESSION RENEWAL IN PMIP4 CASE VIA DHCP REQUEST - DHCP RELAY IN ASN	
30		404
31	FIGURE 4-126 – PMIP4 SESSION RENEWAL PROCEDURE	406
32	FIGURE 4-127 – DHCP SESSION RENEWAL IN PMIP4 CASE- DHCP PROXY IN ASN	407
33	FIGURE 4-128 – DHCP SESSION RENEWAL IN PMIP4 CASE- DHCP RELAY IN ASN	408
34	FIGURE 4-129 – CSN-ANCHORED MOBILITY (PMIP)	416
35	FIGURE 4-130 – PMIP4 SESSION RELEASE TRIGGERED BY MS	420
36	FIGURE 4-131 – PMIP4 SESSION RELEASE TRIGGERED BY ASN	422
37	FIGURE 4-132 – PMIP4 SESSION RELEASE TRIGGERED BY HA	423
38	FIGURE 4-133 – PMIP4 SESSION RELEASE TRIGGERED BY AUTHENTICATOR OR AAA	425
39	FIGURE 4-134 – CSN-ANCHORED MOBILITY (CMIP)	435
40	FIGURE 4-135 – CLIENT MIP6 CONNECTION SETUP PROCEDURE	439
41	FIGURE 4-136 – CSN-ANCHORED MOBILITY HANDOVER	444
42	FIGURE 4-137 - PMIP6 CONNECTION SETUP PROCEDURE THROUGH DHCPV6	454
43	FIGURE 4-138 - PMIP6 CONNECTION SETUP PROCEDURE WITH SLAAC	456
44	FIGURE 4-139 - PMIP6 CONNECTION SETUP FOR AN IPV4 MS	458
45	FIGURE 4-140 - PMIP6 LIFETIME RENEWAL	460
46	FIGURE 4-141 – PMIP6 CSN ANCHORED MOBILITY	463
47	FIGURE 4-142 - PMIP6 SESSION TERMINATION BY MS / MAG	471
48	FIGURE 4-143 - PMIP6 SESSION TERMINATION BY AAA	472
49	FIGURE 4-144 - PMIP6 SESSION TERMINATION BY LMA	473
50	FIGURE 4-145 –RRC-RRC COMMUNICATION ON R6 AND R4	474
51	FIGURE 4-146 – RRC-RRC COMMUNICATION ON R8 (PROVIDED R8 IS AVAILABLE)	475
52	FIGURE 4-147 – PER-BS SPARE CAPACITY REPORTING PROCEDURE	476
53	FIGURE 4-148 – PER-BS SPARE CAPACITY REPORTING PROCEDURE VIA R8	477
54	FIGURE 4-149 – PER-BS RADIO CONFIGURATION REPORTING PROCEDURE	480
55	FIGURE 4-150 – PER-BS RADIO CONFIGURATION UPDATE REPORTING PROCEDURE VIA R8	482
56	FIGURE 4-151 – SECURE LOCATION UPDATE WITH NO PAGING CONTROLLER RELOCATION	487

1	FIGURE 4-152 – SECURE LOCATION UPDATE WITH PAGING CONTROLLER RELOCATION .....	489
2	FIGURE 4-153 – TOPOLOGICALLY AWARE PAGING ANNOUNCE SCHEME .....	498
3	FIGURE 4-154 – TOPOLOGICALLY UNAWARE PAGING ANNOUNCE SCHEME.....	499
4	FIGURE 4-155 – SINGLE-STEP PAGING .....	500
5	FIGURE 4-156 – MULTI-STEP PAGING .....	500
6	FIGURE 4-157 – PAGING PROCEDURE.....	501
7	FIGURE 4-158 – STOP PAGING PROCEDURE .....	503
8	FIGURE 4-159 – IDLE MODE EXIT PROCEDURE .....	509
9	FIGURE 4-160 – IDLE MODE EXIT PROCEDURE WHEN THE MANAGEMENT RESOURCE HOLDING	
10	TIMER HAS NOT EXPIRED AND WHEN THE MS STATE STORED AT THE BS IS NOT	
11	REVOKED BY THE ANCHOR PC .....	514
12	FIGURE 4-161 – MS INITIATED IDLE MODE ENTRY .....	535
13	FIGURE 4-162 – NETWORK INITIATED IDLE MODE ENTRY .....	538
14	FIGURE 4-163 – FA MIGRATION DURING IDLE MODE: ANCHOR PC INITIATED (TRIGGER TO NEW FA)	
15	.....	562
16	FIGURE 4-164 – FA MIGRATION DURING IDLE MODE: ANCHOR PC INITIATED (TRIGGER TO OLD FA)	
17	.....	564
18	FIGURE 4-165 – FA MIGRATION DURING IDLE MODE: NEW (TARGET) FA INITIATED .....	566
19	FIGURE 4-166 – ANCHOR PC-ASN TRIGGERED FA MIGRATION FOR AN IDLE MODE MS IN A PMIP-	
20	ENABLED ASN.....	568
21	FIGURE 4-167 – TARGET ASN (NEW FA) TRIGGERED FA MIGRATION FOR AN IDLE MODE MS IN A	
22	PMIP-ENABLED ASN .....	569
23	FIGURE 4-168 – SIMPLE IP RE-ANCHORING PROCEDURE .....	570
24	FIGURE 4-169 – PMIP6 AR/MAG MIGRATION FOR AN IDLE MODE MS.....	572
25	FIGURE 4-170 – IPV6 NETWORK MODEL .....	574
26	FIGURE 4-171 – IPV6 ADDRESS FORMAT .....	575
27	FIGURE 4-172 – ILLUSTRATION OF FORMING THE IID .....	576
28	FIGURE 4-173 – R4/R6 DATA PATH PRE-REGISTRATION PROCEDURE.....	578
29	FIGURE 4-174 – R6 DATA PATH PRE-REGISTRATION PROCEDURE .....	579
30	FIGURE 4-175 – R4/R6 CONTEXT RETRIEVAL PROCEDURE .....	580
31	FIGURE 4-176 – R6 AUTHENTICATOR CONTEXT RETRIEVAL PROCEDURE .....	581
32	FIGURE 4-177 – R4/R6 DATA PATH REGISTRATION PROCEDURE .....	582
33	FIGURE 4-178 – DATA PATH REGISTRATION PROCEDURE.....	583
34	FIGURE 4-179 – R4/R6 DATA PATH DE-REGISTRATION PROCEDURE.....	584
35	FIGURE 4-180 –PATH DE-REGISTRATION PROCEDURE .....	585
36	FIGURE 4-181 – R4/R6 CMAC KEY COUNT UPDATE PROCEDURE .....	586
37	FIGURE 4-182 – R6 CMAC KEY COUNT UPDATE PROCEDURE .....	587
38	FIGURE 4-183 – MAC CONTEXT RETRIEVAL PROCEDURE .....	588
39	FIGURE 4-184 – EAP NOTIFICATION EXCHANGE .....	589
40	FIGURE 4-185 – RELEASE/CAPABILITY NEGOTIATION PROCEDURE (PUSH OR PULL MODE).....	598
41	FIGURE 4-186 – NETWORK ENTRY WITH R3-R5 VERSION NEGOTIATION PROCEDURE.....	603
42	FIGURE 4-187 – KEEP-ALIVE PROCEDURE.....	607
43	FIGURE 4-188 – AS DISCOVERY (ROAMING SCENARIO) .....	611
44	FIGURE 5-1 – STRUCTURE OF THE DATA INTEGRITY METHOD BITMASK .....	738
45	FIGURE 5-2 – BSN TLV VALUE FIELD FORMAT .....	740
46	FIGURE 5-3 – BSN ARQ STATE BITMAP FORMAT .....	741
47	FIGURE 6-1 – DATA PLANE WITH R4 AND R6 .....	1022
48	FIGURE 6-2 – GRE ENCAPSULATION.....	1023
49	FIGURE 6-3 – GRE HEADER FORMAT .....	1023
50	FIGURE 6-4 – IPOETH-CS LINK MODEL IN THE WIMAX ARCHITECTURE .....	1025
51		
52		

## List of Tables

TABLE 3-1 – PROCESSING OF TLVS, ABNORMAL CASES.....	15
TABLE 3-2 – HANDLING OF MESSAGE FLOW OF TRANSACTIONS, ABNORMAL CASES.....	17
TABLE 4-1 – NSP ID 24-BIT FORMAT FOR NETWORK DISCOVERY AND SELECTION.....	21
TABLE 4-2 – NAP SELECTION POLICY VALUES IN CAPL.....	25
TABLE 4-3 – V-NSP SELECTION POLICY VALUES IN RAPL.....	26
TABLE 4-4 – MOBILITY KEYS GENERATION AND USAGE.....	46
TABLE 4-5 – DHCP KEYS GENERATION AND USAGE.....	52
TABLE 4-6 – FUNCTIONAL BLOCKS FOR DEVICE/USER AUTHENTICATION.....	55
TABLE 4-7 – WIMAX DECORATION AVP DEFINITIONS.....	59
TABLE 4-8 – AR_EAP_START.....	75
TABLE 4-9 – AR_EAP_TRANSFER FROM AUTHENTICATOR TO BS (EAP INITIATION).....	76
TABLE 4-10 – KEY_CHANGE_DIRECTIVE FROM AUTHENTICATOR TO BS.....	78
TABLE 4-11 – KEY_CHANGE_CNF MESSAGE FROM BS TO AUTHENTICATOR (PKMV2 3WHS COMPLETION).....	79
TABLE 4-12 – KEY_CHANGE_ACK.....	80
TABLE 4-13 – RELOCATION_NOTIFY FROM “NEW” AUTHENTICATOR TO “OLD” AUTHENTICATOR.....	82
TABLE 4-14 – RELOCATION_NOTIFY_RSP FROM “OLD” AUTHENTICATOR TO “NEW” AUTHENTICATOR.....	83
TABLE 4-15 – RELOCATION_COMPLETE_REQ MESSAGE FROM “NEW” AUTHENTICATOR TO “OLD” AUTHENTICATOR.....	87
TABLE 4-16 – RELOCATION_COMPLETE_RSP MESSAGE.....	87
TABLE 4-17 – RELOCATION_COMPLETE_ACK.....	91
TABLE 4-18 – RELOCATION_REQ FROM “OLD” AUTHENTICATOR TO “NEW” AUTHENTICATOR.....	92
TABLE 4-19 – RELOCATION_RSP FROM “NEW” AUTHENTICATOR TO “OLD” AUTHENTICATOR.....	96
TABLE 4-20 – CONTEXT_RPT FROM “NEW” AUTHENTICATOR TO ANCHOR DP/FA.....	97
TABLE 4-21 – CONTEXT_ACK FROM ANCHOR DP/FA TO “NEW” AUTHENTICATOR.....	97
TABLE 4-22 – TIMERS AND TIMING CONSIDERATIONS.....	98
TABLE 4-23 – ERROR HANDLING SCENARIOS.....	98
TABLE 4-24 – ACTIONS AFTER TIMER MAX RETRY.....	99
TABLE 4-25 – LIST OF AUTHENTICATION RELAY PROTOCOL MESSAGES.....	102
TABLE 4-26 – AUTHENTICATION RELAY MESSAGES MAPPING TO PKMV2 AND VICE VERSA.....	103
TABLE 4-27 – RELATION OF SUBSCRIBER AND SUBSCRIPTION.....	104
TABLE 4-28 – ACCOUNTING MODES.....	105
TABLE 4-29 – INTERPRETATION OF ACCOUNTING- REQUEST PACKETS.....	123
TABLE 4-30 – UDR RECORD STRUCTURE.....	124
TABLE 4-31 – CONTEXT_RPT FROM ACCOUNTING AGENT TO “OLD” ACCOUNTING CLIENT.....	132
TABLE 4-32 – RR_REQ (CREATE) / HO_REQ / ANCHOR_DPF_HO_REQ (FOR R4 ONLY) / CONTEXT_RPT / IM_EXIT_STATE_CHANGE_RSP MESSAGE STRUCTURE.....	144
TABLE 4-33 – RR_RSP (MODIFY AND DELETE) MESSAGE STRUCTURE.....	145
TABLE 4-34 – BULK INTERIM UPDATE MESSAGE STRUCTURE.....	146
TABLE 4-35 – PATH_DEREG_REQ / IM_ENTRY_STATE_CHANGE_REQ / NETEXIT_MS_STATE_CHANGE_REQ/RSP MESSAGE STRUCTURE.....	148
TABLE 4-36 – PREPAID_REQUEST MESSAGE STRUCTURE.....	150
TABLE 4-37 – PREPAID_NOTIFY MESSAGE STRUCTURE.....	151
TABLE 4-38 – TIMER VALUES FOR PREPAID MESSAGES OVER R4.....	152
TABLE 4-39 – TIMER MAX RETRY CONDITIONS.....	152
TABLE 4-40 – HOTLINING_REQ [PPC TO HLD].....	152
TABLE 4-41 – HOTLINING_RSP [HLD TO PPC].....	153
TABLE 4-42 – MS_PREATTACHMENT_REQ FROM BS TO AUTHENTICATOR.....	167
TABLE 4-43 – MS_PREATTACHMENT_RSP FROM AUTHENTICATOR TO BS.....	169
TABLE 4-44 – MS_PREATTACHMENT_ACK FROM BS TO AUTHENTICATOR.....	170
TABLE 4-45 – AR_EAP_TRANSFER FROM AUTHENTICATOR TO BS (EAP INITIATION).....	170
TABLE 4-46 – MS_ATTACHMENT_REQ FROM BS TO AUTHENTICATOR.....	173
TABLE 4-47 – MS_ATTACHMENT_RSP FROM AUTHENTICATOR TO BS.....	175

1	TABLE 4-48 – TIMER VALUES FOR INITIAL NETWORK ENTRY PROCEDURE .....	177
2	TABLE 4-49 – INITIAL NETWORK ENTRY – HANDLING ERROR CONDITIONS .....	178
3	TABLE 4-50 – TIMER MAX RETRY CONDITIONS .....	179
4	TABLE 4-51 – PATH_DEREG_REQ MESSAGE IN MS NETWORK EXIT PROCEDURE .....	204
5	TABLE 4-52 – NETEXIT MS STATE CHANGE REQ MESSAGE COMPOSITION .....	205
6	TABLE 4-53 – NETEXIT MS STATE CHANGE_RSP MESSAGE COMPOSITION .....	206
7	TABLE 4-54 – NETWORK EXIT TIMER VALUES FOR R4 AND R6 .....	207
8	TABLE 4-55 – ACTIONS AFTER TIMER MAX RETRY .....	207
9	TABLE 4-56 – TIMER VALUES FOR SF MANAGEMENT PROCEDURE .....	226
10	TABLE 4-57 – TIMER MAX RETRY CONDITIONS .....	227
11	TABLE 4-58 – DATA PATH CONTROL MESSAGES .....	229
12	TABLE 4-59 – RR_REQ: SF CREATION OR MODIFICATION (ANCHOR-SFA TO SERVING-SFA) .....	229
13	TABLE 4-60 – RR_REQ: SF CREATION (SERVING-SFA TO ANCHOR-SFA) .....	232
14	TABLE 4-61 – RR_REQ: SF MODIFICATION, STATE CHANGE ONLY (SERVING-SFA TO ANCHOR-SFA) .....	235
15	TABLE 4-62 – RR_REQ: SF MODIFICATION (SERVING-SFA TO ANCHOR-SFA) .....	235
16	TABLE 4-63 – RR_REQ: DELETION OF A SF .....	238
17	TABLE 4-64 – RR_RSP: SF CREATION .....	238
18	TABLE 4-65 – RR_RSP: DELETION OF A SF .....	240
19	TABLE 4-66 – RR_ACK .....	240
20	TABLE 4-67 – PATH-REG-REQ: CREATION OF SF AND DP (NETWORK INITIATED) .....	241
21	TABLE 4-68 – PATH-REG-REQ: CREATION OF SF AND DP (MS INITIATED) .....	245
22	TABLE 4-69 – PATH-REG-RSP: CREATION OF SF AND DP (NETWORK INITIATED) .....	248
23	TABLE 4-70 – PATH-REG-RSP: CREATION OF SF AND DP (MS INITIATED) .....	251
24	TABLE 4-71 – PATH-REG-ACK: CREATION OF SF AND DP .....	253
25	TABLE 4-72 – PATH-MODIFICATION-REQ: MODIFICATION OF SF AND DP .....	254
26	TABLE 4-73 – PATH-MODIFICATION-RSP: MODIFICATION OF SF AND DP .....	258
27	TABLE 4-74 – PATH-MODIFICATION-ACK: MODIFICATION OF SF AND DP .....	261
28	TABLE 4-75 – PATH_DEREG_REQ: DELETION OF SF AND DP .....	261
29	TABLE 4-76 – PATH_DEREG_RSP: DELETION OF SERVICE FLOW AND DP .....	262
30	TABLE 4-77 – PATH_DEREG_ACK: DELETION OF SERVICE FLOW AND DP .....	262
31	TABLE 4-78 – HO PREPARATION PHASE TIMER VALUES FOR R4 .....	277
32	TABLE 4-79 – TIMER MAX RETRY CONDITIONS .....	277
33	TABLE 4-80 – HO ACTION PHASE R4 AND R6 TIMER VALUES .....	297
34	TABLE 4-81 – ACTIONS AFTER MAX RE-TRANSMIT RETRIES .....	298
35	TABLE 4-82 – HO_REQ .....	303
36	TABLE 4-83 – CONTEXT_REQ FROM TARGET BS TO AUTHENTICATOR ASN-GW .....	313
37	TABLE 4-84 – CONTEXT_RPT FROM AUTHENTICATOR ASN-GW TO TARGET BS .....	313
38	TABLE 4-85 – HO_RSP .....	314
39	TABLE 4-86 – HO_ACK .....	316
40	TABLE 4-87 – PATH_PREREG_REQ .....	317
41	TABLE 4-88 – PATH_PREREG_RSP .....	318
42	TABLE 4-89 – PATH_PREREG_ACK .....	318
43	TABLE 4-90 – HO_CNF (HO CONFIRM TYPE IS CONFIRM OR UNCONFIRMED) .....	319
44	TABLE 4-91 – HO_CNF (HO CONFIRM TYPE IS CANCEL OR REJECT) .....	326
45	TABLE 4-92 – CONTEXT_REQ FROM TARGET BS TO SERVING BS .....	327
46	TABLE 4-93 – CONTEXT_RPT FROM SERVING BS TO TARGET BS .....	327
47	TABLE 4-94 – PATH_REG_REQ .....	336
48	TABLE 4-95 – PATH_REG_RSP .....	336
49	TABLE 4-96 – PATH_REG_ACK .....	337
50	TABLE 4-97 – CMAC_KEY_COUNT_UPDATE .....	337
51	TABLE 4-98 – CMAC_KEY_COUNT_UPDATE_ACK .....	338
52	TABLE 4-99 – HO COMPLETE .....	338
53	TABLE 4-100 – HO PREPARATION PHASE TIMER VALUES FOR HO MESSAGES OVER R8 .....	342
54	TABLE 4-101 – TIMER MAX RETRY CONDITIONS .....	342
55	TABLE 4-102 – HO ACTION PHASE TIMER VALUES FOR R8 .....	350



1	TABLE 4-103 – TIMER MAX RETRY CONDITIONS .....	350
2	TABLE 4-104 –INFO IN HO_REQ.....	369
3	TABLE 4-105 – SWITCHING DATA PATH ID & SDU INFO IN PATH PRE-REG_REQ/RSP .....	370
4	TABLE 4-106 – SDU INFO IN HO_CNF OR CONTEXT_RPT FROM SERVING BS TO TARGET BS.....	371
5	TABLE 4-107 – SDU SN IN PATH_DE-REG REQ FROM SERVING ASN GW TO SERVING BS, ANCHOR	
6	ASN-GW TO SERVING BS .....	371
7	TABLE 4-108 – .....	372
8	TABLE 4-109 – DATA INTEGRITY MINI-HEADER .....	378
9	TABLE 4-110 – ADDITIONS HO_CNF OR CONTEXT RPT FROM SERVING BS TO TARGET BS.....	384
10	TABLE 4-111 – DATA INTEGRITY METHOD TLV IN PATH_PRE-REG_REQ AND HO REQ .....	386
11	TABLE 4-112 – DATA INTEGRITY METHOD TLV IN PATH_PRE-REG_RSP AND HO RSP .....	387
12	TABLE 4-113 – ANCHOR_DPF_HO_REQ MESSAGE.....	409
13	TABLE 4-114 – ANCHOR_DPF_HO_TRIGGER MESSAGE.....	412
14	TABLE 4-115 – ANCHOR_DPF_HO_RSP MESSAGE.....	413
15	TABLE 4-116– CONTEXT_RPT FROM TARGET FA TO SERVING BS .....	413
16	TABLE 4-117– CONTEXT_ACK FROM SERVING BS TO TARGET FA.....	413
17	TABLE 4-118 – ANCHOR_DPF_RELOCATE_REQ MESSAGE.....	414
18	TABLE 4-119 – FA_REGISTER_REQ MESSAGE .....	414
19	TABLE 4-120 – FA_REGISTER_RSP MESSAGE .....	415
20	TABLE 4-121 – ANCHOR_DPF_RELOCATE_RSP MESSAGE.....	415
21	TABLE 4-122 – TIMER VALUES FOR PMIP4 CSN MM HANDOVER MESSAGES OVER R4/R3 .....	418
22	TABLE 4-123 – TIMER MAX RETRY CONDITIONS .....	418
23	TABLE 4-124 – FA_REVOKE_REQ .....	419
24	TABLE 4-125 – FA_REVOKE_RSP.....	420
25	TABLE 4-126 – TIMER VALUES FOR MS INITIATED PMIP4 SESSION RELEASE MESSAGES OVER R4/R3	
26	.....	421
27	TABLE 4-127 – TIMER MAX RETRY CONDITIONS .....	421
28	TABLE 4-128 – TIMER VALUES FOR ASN INITIATED PMIP4 SESSION RELEASE MESSAGES OVER	
29	R4/R3 .....	422
30	TABLE 4-129 – TIMER MAX RETRY CONDITIONS .....	423
31	TABLE 4-130 – TIMER VALUES FOR HA INITIATED PMIP4 SESSION RELEASE MESSAGES .....	424
32	TABLE 4-131 – TIMER MAX RETRY CONDITIONS .....	424
33	TABLE 4-132 – TIMER MAX RETRY CONDITIONS .....	426
34	TABLE 4-133 – ANCHOR_DPF_HO_REQ MESSAGE.....	433
35	TABLE 4-134 – TIMER VALUES FOR CMIP4 CSN MM HANDOVER MESSAGES OVER R4/R3.....	437
36	TABLE 4-135 – TIMER MAX RETRY CONDITIONS .....	437
37	TABLE 4-136 – GUIDELINES FOR USING RFC 4285 FOR PMIP6 .....	449
38	TABLE 4-137 – ANCHOR_DPF_HO_REQ MESSAGE.....	464
39	TABLE 4-138 – ANCHOR_DPF_RELOCATE_REQ FROM TARGET ASN TO AUTHENTICATOR ASN.....	467
40	TABLE 4-139 – ANCHOR_DPF_RELOCATE_RSP FROM AUTHENTICATOR ASN TO TARGET ASN.....	468
41	TABLE 4-140 – ANCHOR_DPF_RELOCATE_ACK FROM TARGET ASN TO AUTHENTICATOR ASN .....	468
42	TABLE 4-141 – TIMER VALUES FOR PMIP6 CSN MM HANDOVER MESSAGES OVER R4/R3 .....	468
43	TABLE 4-142 – TIMER MAX RETRY CONDITIONS .....	469
44	TABLE 4-143 – RRM PROCEDURES, MESSAGES, MAPPING TO REFERENCE POINTS .....	475
45	TABLE 4-144 – SPARE_CAPACITY_REQ.....	478
46	TABLE 4-145 – SPARE_CAPACITY_RPT.....	479
47	TABLE 4-146 – RADIO_CONFIG_UPDATE_REQ .....	483
48	TABLE 4-147 – RADIO_CONFIG_UPDATE_RPT.....	484
49	TABLE 4-148 – RADIO_CONFIG_UPDATE_ACK.....	485
50	TABLE 4-149 – RRM CONFIGURATION REPORT TIMER.....	485
51	TABLE 4-150 – RRM-CONFIG-RPT TIMER VALUES .....	486
52	TABLE 4-151 – LOCATION UPDATE TIMER VALUES .....	492
53	TABLE 4-152 – TIMER MAX RETRY CONDITIONS .....	492
54	TABLE 4-153 – LU_REQ PRIMITIVE STRUCTURE.....	494
55	TABLE 4-154 – LU_RSP PRIMITIVE STRUCTURE .....	494
56	TABLE 4-155 – LU_CNF PRIMITIVE STRUCTURE.....	496

1	TABLE 4-156 – CONTEXT_REQ PRIMITIVE STRUCTURE .....	496
2	TABLE 4-157 – CONTEXT_RPT PRIMITIVE STRUCTURE .....	496
3	TABLE 4-158 – PC_RELOCATION_IND PRIMITIVE STRUCTURE .....	497
4	TABLE 4-159 – PC_RELOCATION_ACK PRIMITIVE STRUCTURE .....	497
5	TABLE 4-160 – PAGING TIMER VALUES FOR R4 AND R6 .....	504
6	TABLE 4-161 – TIMER MAX RETRY CONDITIONS .....	505
7	TABLE 4-162 – R4 INITIATE_PAGING_REQ .....	505
8	TABLE 4-163 – R4 INITIATE_PAGING_RSP .....	505
9	TABLE 4-164 – R4 PAGING_ANNOUNCE .....	506
10	TABLE 4-165 – R6 PAGING_ANNOUNCE .....	507
11	TABLE 4-166 – TIMER VALUES FOR IM EXIT MESSAGES OVER R4 .....	512
12	TABLE 4-167 – TIMER MAX RETRY CONDITIONS .....	512
13	TABLE 4-168 – TIMER VALUES FOR IM EXIT MESSAGES OVER R4 .....	515
14	TABLE 4-169 – TIMER MAX RETRY CONDITIONS .....	516
15	TABLE 4-170 – IM_EXIT_STATE_CHANGE_REQ OVER R6 .....	516
16	TABLE 4-171 – IM_EXIT_STATE_CHANGE_RSP OVER R6 .....	516
17	TABLE 4-172 – PATH_REG_ACK OVER R6 .....	525
18	TABLE 4-173 – IM_EXIT_STATE_CHANGE_REQ OVER R4 .....	525
19	TABLE 4-174 – IM_EXIT_STATE_CHANGE_RSP OVER R4 .....	525
20	TABLE 4-175 – IM_EXIT_STATE_IND .....	533
21	TABLE 4-176 – IM_EXIT_STATE_IND_ACK .....	533
22	TABLE 4-177 – PATH_REG_ACK OVER R4 .....	534
23	TABLE 4-178 – CONTEXT_REQ OVER R4 .....	534
24	TABLE 4-179 – CONTEXT_RPT OVER R4 .....	534
25	TABLE 4-180 – IDLE MODE ENTRY TIMER VALUES .....	541
26	TABLE 4-181 – TIMER MAX RETRY CONDITIONS .....	541
27	TABLE 4-182 – IM_ENTRY_STATE_CHANGE_REQ OVER R6 .....	543
28	TABLE 4-183 –ANCHOR_PC_IND .....	551
29	TABLE 4-184 –ANCHOR_PC_ACK .....	551
30	TABLE 4-185 – IM_ENTRY_STATE_CHANGE_REQ OVER R4 .....	551
31	TABLE 4-186 – IM_ENTRY_STATE_CHANGE_RSP .....	559
32	TABLE 4-187 – IM_ENTRY_STATE_CHANGE_ACK .....	560
33	TABLE 4-188 – CONTEXT_RPT FROM ANCHOR ASN (OLD) TO ANCHOR PC FOR PMIP6 IM HANDOVER .....	573
34	.....	573
35	TABLE 4-189 – TYPE-DATA FIELD OF THE EAP NOTIFICATION REQUEST PACKET .....	589
36	TABLE 4-190 – CAPABILITY_REQ .....	600
37	TABLE 4-191 – CAPABILITY_RSP .....	601
38	TABLE 4-192 – CAPABILITY_ACK .....	602
39	TABLE 4-193 – KEEP-ALIVE_REQ .....	608
40	TABLE 4-194 – KEEP-ALIVE_RSP .....	609
41	TABLE 5-1 – FUNCTION AND MESSAGE TYPES INDEX .....	612
42	TABLE 5-2 – MEANINGS OF THE BITS .....	739
43	TABLE 5-3 – SCOPE VALUES DEFINED .....	740
44	TABLE 5-4 – ARQ STATE VALUES .....	741
45	TABLE 5-5 – RADIUS MESSAGES BETWEEN NAS AND HAAA .....	764
46	TABLE 5-6 – RADIUS COA MESSAGES BETWEEN NAS AND HAAA .....	770
47	TABLE 5-7 – RADIUS MESSAGES BETWEEN ASN AND HAAA FOR BOOTSTRAPPING MOBILITY .....	771
48	SERVICE .....	771
49	TABLE 5-8 – RADIUS ATTRIBUTES BETWEEN ASN AND HAAA FOR DHCP RELAY .....	773
50	TABLE 5-9 – RADIUS MESSAGES BETWEEN HA AND HAAA .....	775
51	TABLE 5-10 – RADIUS MESSAGES BETWEEN LMA AND HAAA .....	778
52	TABLE 5-11 – RADIUS MESSAGES BETWEEN DHCP SERVER AND HAAA .....	780
53	TABLE 5-12 – RADIUS ACCESS-ACCEPT (FROM HAAA TO HLD) .....	781
54	TABLE 5-13 – RADIUS COA (FROM HAAA TO HLD) .....	781
55	TABLE 5-14 – RADIUS DISCONNECT NACK MESSAGE .....	791
56	TABLE 5-15 – SHOWING VALID QOS ATTRIBUTES FOR EACH SCHEDULE-TYPE .....	813

1	TABLE 5-16 – COMMANDS OF WIMAX NETWORK ACCESS AUTHENTICATION AND	
2	AUTHORIZATION DIAMETER APPLICATION .....	878
3	TABLE 5-17 – WDER COMMAND IN CASE OF INITIAL AUTHENTICATION .....	880
4	TABLE 5-18 – WDER COMMAND WHEN SENT IN RESPONSE TO DEA WITH RESULT-CODE	
5	DIAMETER_MULTI_ROUND_AUTH .....	882
6	TABLE 5-19 – WDER COMMAND WHEN REQUEST-TYPE IS AUTHENTICATE_ONLY .....	883
7	TABLE 5-20 – ATTRIBUTES OF THE WDER COMMAND .....	884
8	TABLE 5-21 – WDEA COMMAND WHEN RESULT-CODE IS DIAMETER_MULTI_ROUND_AUTH .....	887
9	TABLE 5-22 – WDEA COMMAND WHEN RESULT-CODE IS DIAMETER_SUCCESS .....	889
10	TABLE 5-23 – ATTRIBUTES OF THE WDEA COMMAND .....	893
11	TABLE 5-24 – ATTRIBUTES OF THE WCAR COMMAND .....	895
12	TABLE 5-25 – ATTRIBUTES OF THE WCAA COMMAND .....	896
13	TABLE 5-26 – ATTRIBUTES OF THE WRAR COMMAND .....	899
14	TABLE 5-27 – ATTRIBUTES OF THE WRAA COMMAND .....	901
15	TABLE 5-28 – ATTRIBUTES OF THE WSTR COMMAND .....	903
16	TABLE 5-29 – ATTRIBUTES OF THE WSTA COMMAND .....	904
17	TABLE 5-30 – ATTRIBUTES OF THE WASR COMMAND .....	906
18	TABLE 5-31 – ATTRIBUTES OF THE WASA COMMAND .....	908
19	TABLE 5-32 – ATTRIBUTES OF THE WHA4R COMMAND .....	911
20	TABLE 5-33 – ATTRIBUTES OF THE WHA4A COMMAND .....	914
21	TABLE 5-34 – ATTRIBUTES OF THE WHA6R COMMAND .....	917
22	TABLE 5-35 – ATTRIBUTES OF THE WHA6A COMMAND .....	919
23	TABLE 5-36 – ATTRIBUTES OF THE WDHCP R COMMAND .....	921
24	TABLE 5-37 – ATTRIBUTES OF THE WDHCP A COMMAND .....	922
25	TABLE 5-38 – CREDIT-CONTROL-REQUEST MESSAGE CONTENT .....	924
26	TABLE 5-39 – CREDIT-CONTROL-ANSWER MESSAGE CONTENT .....	930
27	TABLE 5-40 –R3-OC SPECIFIC AVPS .....	934
28	TABLE 5-41 –R3-OC RE-USED DIAMETER AVPS .....	935
29	TABLE 5-42 – IETF REUSED AVPS .....	942
30	TABLE 5-43 – 3GPP REUSED AVPS .....	943
31	TABLE 5-44 – WIMAX SPECIFIC AVPS .....	943
32	TABLE 5-45 – AVP OCCURRENCE TABLE .....	945
33	TABLE 5-46 – SHOWING VALID QOS ATTRIBUTES FOR EACH SCHEDULE-TYPE .....	957
34	TABLE 5-47 – PBU/PBA FIELDS AND OPTIONS .....	1014
35	TABLE 5-48 – BRI/BRA FIELDS AND OPTIONS .....	1016
36	TABLE 6-1 – GRE HEADER FIELD DEFINITIONS .....	1024
37	TABLE 7-1 – FEATURE LIST FOR NWG REL 1.5 .....	1026

38

## 1 **Revision History**

November 6, 2009	Initial version of Release 1.5.
---------------------	---------------------------------

2

---

# 1. Introduction and Scope

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

## 1.1 Relationship between Stage 2 and Stage 3

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

- Procedures, call flows, messages, timers, TLVs and attributes are specified, based on the framework in Stage 2.
- Whereas Stage 2 is a functional specification, Stage 3 describes normative mapping of procedures and messages. Wherever applicable, mandatory and optional messages and parameters are defined in this document.

## 1.2 Scope

This is Release 1.5 of the NWG specification. In this Release, the specification covers stationary and mobile WiMAX clients connecting to a mobile WiMAX network. The specification is based on Stage 1 requirements from the SPWG. This document is the basis for NWIoT specifications.

## 1.3 Terminology

### 1.3.1 Terms

ASN control protocol	The common protocol on ASN reference points R4, R6 and R8.
Legacy node	A network node that conforms to a version of this specification prior to version 1.3.
Reserved bit	A reserved bit is set to 0 by the sender and ignored by the receiver, see section 5.3.2.
Reserved value	A reserved value SHALL NOT be used by the sender; the receiver SHALL consider a reserved value as erroneous, see section 5.3.2.
Skip a message	Not take any ASN control protocol related action.

### 1.3.2 Conventions

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

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

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

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

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

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

---

## 2. References

- [1] T32-001-R015 and T33-004-R015, WiMAX Forum™ Network Architecture, Architecture Tenets, Reference Model and Reference Points; Base Specification and Informal Annex
- [2] T33-004-R015, WiMAX Forum™ Network Architecture, Informative Annex: Hooks and Principles for Evolution
- [3] T33-109-R015, WiMAX Forum™ Network Architecture, Policy and Charging Control
- [4] WiMAX Forum SPWG, Recommendations and Requirements for Networks based on WiMAX Forum Certified™ Products, Release 1.5, October 18, 2007 [SPWGR1.5]
- [5] T33-102-R015v02, WiMAX Forum™ Network Architecture, Emergency Services Support
- [6] T33-103-R015v04, WiMAX Forum™ Network Architecture, Architecture, detailed Protocols and Procedures, WiMAX Over-The-Air General Provisioning System Specification
- [7] T33-104-R015, WiMAX Forum™ Network Architecture, Detailed Protocols and Procedures, WiMAX Over-The-Air Provisioning & Activation Protocol based on OMA DM Specifications
- [8] T33-108-R015, WiMAX Forum™ Network Architecture, Robust Header Compression (ROHC) Support
- [9] T33-112-R015, WiMAX Forum™ Network Architecture, System Requirements, Network Protocols and Architecture for Multi-cast Broad-cast Services, Dynamic Service Flow Based (MCBCS – DSx).
- [10] 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.
- [11] IEEE 802.16e-2005 March 2006, Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands
- [12] IEEE 802.16g draft
- [13] IEEE Std 802.16™-2009, IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Broadband Wireless Access Systems, 29 May 2009 (Revision of IEEE Std 802.16-2004)
- [14] ITU-T Rec. E.212, The international identification plan for mobile terminals and mobile users
- [15] "Layer 2 Relay Agent Information", Bharat Joshi, Pavan Kurapati, 16-May-08, <draft-ietf-dhc-l2ra-01.txt>
- [16] EAP-AKA, J. Arkko et al, Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA), RFC4187
- [17] [EAP-TLS, B. Aboba and D. Simon, PPP EAP TLS Authentication Protocol \(EAP-TLS\), RFC5216](#)
- [18] EAP-TTLS, Paul, Funk, EAP Tunneled TLS Authentication Protocol (EAP-TTLS), draft-ietf-pppext-eap-ttls-05
- [19] MSCHAPv2, G. Zorn, Microsoft PPP CHAP Extensions, Version 2, RFC2759
- [20] [RFC 791](#), Internet Protocol
- [21] [RFC 815](#), IP datagram reassembly algorithms
- [22] [RFC 966](#), Host Groups: A Multicast Extension to the Internet Protocol
- [23] [RFC 2104](#), HMAC: Keyed-Hashing for Message Authentication
- [24] [RFC 2131](#), Dynamic Host Configuration Protocol
- [25] [RFC 2132](#), DHCP Options and BOOTP Vendor Extensions

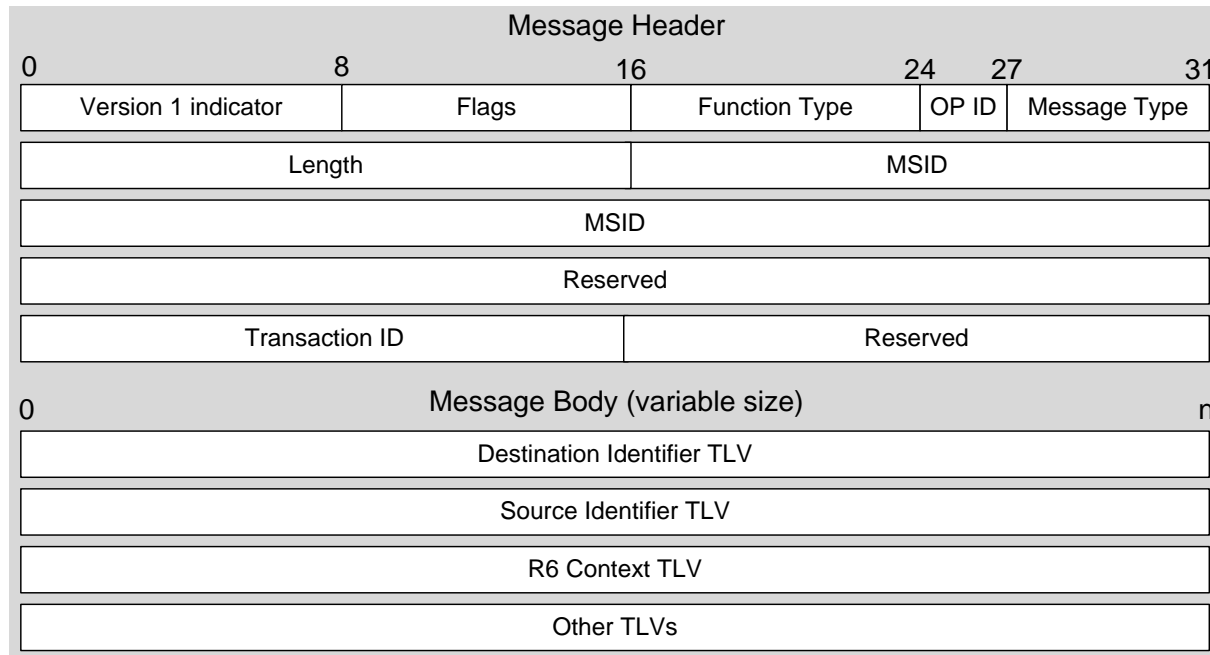
- 1 [26] [RFC 2461, Neighbor Discovery for IP Version 6 \(IPv6\)](#)
- 2 [27] [RFC 2462, IPv6 Stateless Address Autoconfiguration](#)
- 3 [28] [RFC 2473, Generic Packet Tunneling in IPv6](#)
- 4 [29] [RFC 2474](#), Definition of the Differentiated Services Field (DS Field) in the Ipv4 and Ipv6 Headers
- 5 [30] [RFC 2475](#), An Architecture for Differentiated Services
- 6 [31] [RFC 2494](#), Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type
- 7 [32] [RFC 2548](#), Microsoft Vendor-specific RADIUS Attributes
- 8 [33] [RFC 2560](#), X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP
- 9 [34] [RFC 2597](#), Assured Forwarding PHB Group
- 10 [35] [RFC 2780, IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers](#)
- 11 [36] [RFC 2784, Generic Routing Encapsulation \(GRE\)](#)
- 12 [37] [RFC 2865](#), Remote Authentication Dial In User Service (RADIUS)
- 13 [38] [RFC 2866](#), RADIUS Accounting
- 14 [39] [RFC 2868](#), RADIUS Attributes for Tunnel Protocol Support
- 15 [40] [RFC 2869](#), RADIUS Extensions
- 16 [41] [RFC 2890, Key and Sequence Number Extensions to GRE](#)
- 17 [42] [RFC 3012](#), Mobile IPv4 Challenge/Response Extensions
- 18 [43] [RFC 3041](#), Privacy Extensions for Stateless Address Autoconfiguration in Ipv6
- 19 [44] [RFC 3046](#), DHCP Relay Agent Information Option
- 20 [45] [RFC 3162, RADIUS and IPv6](#)
- 21 [46] [RFC 3246](#), An Expedited Forwarding PHB (Per-Hop Behavior)
- 22 [47] [RFC 3315](#), Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- 23 [48] [RFC 3344](#), IP Mobility Support for IPv4
- 24 [49] [RFC 3513, Internet Protocol Version 6 \(IPv6\) Addressing Architecture](#)
- 25 [50] [RFC 3543, Registration Revocation in Mobile Ipv4](#)
- 26 [51] [RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service \(RADIUS\)](#)
- 27 [52] [RFC 3579, RADIUS \(Remote Authentication Dial In User Service\) Support For Extensible Authentication](#)
- 28 [Protocol \(EAP\)](#)
- 29 [53] RFC 3587, IPv6 Global Unicast Address Format
- 30 [54] [RFC 3588, Diameter Base Protocol](#)
- 31 [55] [RFC 3736, Stateless Dynamic Host Configuration Protocol \(DHCP\) Service for IPv6](#)
- 32 [56] [RFC 3748, Extensible Authentication Protocol \(EAP\)](#)
- 33 [57] [RFC 3775, Mobility Support in IPv6](#)
- 34 [58] [RFC 3879, Deprecating Site Local Addresses](#)
- 35 [59] [RFC 3957, Authentication, Authorization, and Accounting \(AAA\) Registration Keys for Mobile IPv4, C.](#)
- 36 [Perkins and P. Calhoun, March 2005, Standards Track](#)
- 37 [60] [RFC 3993, Subscriber-ID Suboption for the Dynamic Host Configuration Protocol \(DHCP\) Relay Agent](#)
- 38 [Option](#)

- 1 [61] [RFC 4004, Diameter Mobile IPv4 Application](#)
- 2 [62] [RFC 4005, Diameter Network Access Server Application](#)
- 3 [63] [RFC 4006, Diameter Credit-Control Application](#)
- 4 [64] [RFC 4017, Extensible Authentication Protocol \(EAP\) Method Requirements for Wireless LANs](#)
- 5 [65] [RFC 4030, The Authentication Suboption for the Dynamic Host Configuration Protocol \(DHCP\) Relay Agent Option](#)
- 6
- 7 [66] [RFC 4072, Diameter Extensible Authentication Protocol \(EAP\) Application](#)
- 8 [67] [RFC 4193, Unique Local IPv6 Unicast Addresses](#)
- 9 [68] [RFC 4282, The Network Access Identifier](#)
- 10 [69] [RFC 4283, Mobile Node Identifier Option for Mobile IPv6 \(MIPv6\)](#)
- 11 [70] [RFC 4284, Identity Selection Hints for the Extensible Authentication Protocol \(EAP\)](#)
- 12 [71] [RFC 4285, Authentication Protocol for Mobile IPv6](#)
- 13 [72] [RFC 4291, IP Version 6 Addressing Architecture](#)
- 14 [73] [RFC 4366, Transport Layer Security \(TLS\) Extensions](#)
- 15 [74] [RFC 4372, Chargeable User Identity](#)
- 16 [75] [RFC 4541, Considerations for Internet Group Management Protocol \(IGMP\) and Multicast Listener Discovery \(MLD\) Snooping Switches](#)
- 17
- 18 [76] [RFC 4595, Use of IKEv2 in the Fibre Channel Security Association Management Protocol](#)
- 19 [77] [RFC 4849, RADIUS Filter Rule Attribute](#)
- 20 [78] [RFC 4862, IPv6 Stateless Address Autoconfiguration](#)
- 21 [79] [RFC 5019, The Lightweight Online Certificate Status Protocol \(OCSP\) Profile for High-Volume Environments](#)
- 22
- 23 [80] [RFC 5121, Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks](#)
- 24 [81] RFC 5213, Proxy Mobile IPv6
- 25 [82] RFCaaaa – draft-adrangi-eap-network-discovery-14.txt, Network Discovery and Selection within the EAP Framework, F. Adrangi, et al., August 2005, Informational (RFC Editor’s Queue)
- 26
- 27 [83] [draft-ietf-16ng-ip-over-ethernet-over-802-dot-16-08.txt](#)
- 28 [84] Draft-ietf-dime-mip6-split-12.txt
- 29 [85] Draft-ietf-dime-qos-attributes-11.txt
- 30 [86] draft-ietf-eap-netsel-problem-05.txt
- 31 [87] draft-ietf-mip4-gen-ext-01.txt
- 32 [88] draft-ietf-mip6-hiopt-12.txt
- 33 [89] draft-ietf-pppext-eap-ttls-05.txt
- 34 [90] draft-ietf-radext-ieee802-00.txt
- 35 [91] draft-yegani-gre-key-extension-03.txt (within a week)
- 36 [92] draft-leung-mip4-proxy-mode-08.txt
- 37 [93] Internet-Draft “IPv4 Support for Proxy Mobile IPv6” (draft-ietf-netlmm-pmip6-ipv4-support-09)
- 38 [94] Internet-Draft “GRE Key Option for Proxy Mobile IPv6” (draft-ietf-netlmm-grekey-option-06)



- 1 [95] Internet-Draft “Binding Revocation for IPv6 Mobility” (draft-ietf-mext-binding-revocation-03)
- 2 [96] draft-ietf-geopriv-radius-lo-23.txt
- 3 [97] Internet-Draft [“Prepaid Extensions to Remote Authentication Dial-In User Service \(RADIUS\)”](#)“ draft-lior-
- 4 [radius-prepaid-extensions-16](#)
- 5 [98] 3GPP TS29.212 “Policy and Charging Control over Gx reference point”, Release 7
- 6 [99] 3GPP TS 32.299 “Charging management; Diameter charging applications”, Release 7
- 7 [100] 3GPP TS 32.240 “Charging architecture and principles”, Release 7
- 8





**Figure 3-2 – Message Format**

All the fields in the message header are mandatory. The bit ordering depicted in the figure refers to network transmit bit order.

The fields have the following meaning:

- Version 1 indicator: This field is 1-byte long. Bit 7 SHALL be set to 1 by the sender. Bits zero to six SHALL be set to 0 by the sender. The receiver SHALL ignore the value in the field.
- Flags: 1 byte long.



**Figure 3-3 – Flags Format**

- R: Restart Next Expected Transaction ID.
- T: The sender SHALL set this bit to 1 if, and only if the message is sent in Relay mode of operation (see section 3.1.1). If this bit is set, Source and Destination Identifier TLVs are included in the message as shown in Figure 3-4.
- S: Used to recognize legacy nodes (see section 1.3.1). S = 0 means the sender is a legacy node, S = 1 means the sender is not a legacy node.
- C: If this bit is set to 1, comprehension is required (cf. section 3.5.1.1) for all of the following three fields in the header
  - a) for the Function type;
  - b) for the OP ID;
  - c) for the Message Type;

If this bit is set to 0, comprehension is not required for any of these three fields.

- E: If this bit is set to 1, the message is an Error Reflection message (see section 3.5.2); if this bit is not set to 1, the message is not an Error Reflection message.
  - r: Reserved bits, SHALL be set to zero by the sender. Receiver SHALL ignore all ‘r’ bits.
  - Function Type: This field is 1 byte long and indicates individual functions, for example, HO Control.
  - OP ID: This field is 3 bits long and indicates Operation Type, as follows:
    - 000: Reserved value. If this value is present, the receiver SHALL diagnose a 'Message Header Failure' error with attribute 'invalid OP ID'. If comprehension is required for the OP ID, the receiver SHALL report the error (cf. section 3.5.2) and otherwise skip the message (cf. section 3.5.1). If comprehension is not required for the OP ID, the receiver SHALL skip the message (cf. section 3.5.1).
    - 001: Request/Initiation (start of 2-way transaction with a Request message or 3-way transaction)
    - 010: Response (response to Request/Initiation)
    - 011: Ack (finishes 3-way transaction or acknowledges an indication message)
    - 100: Indication (1-way transaction, or start of a 2-way transaction with an Indication message if followed by an Ack)
    - 101, 110, 111: reserved values; if one of these values is present, the receiver SHALL diagnose a 'Message Header Failure' error with attribute 'invalid OP ID'. If comprehension is required for the OP ID, the receiver SHALL report the error (cf. section 3.5.2) and otherwise skip the message (cf. section 3.5.1). If comprehension is not required for the OP ID, the receiver SHALL skip the message (cf. section 3.5.1).
  - 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 by the sender; the receiver SHALL ignore all bits.
  - 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 in all (i.e. 1-, 2- and 3-way) transactions, and 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, R6\_Context\_ID}, where R6\_Context\_ID SHALL be taken into account if present, where Source is the originator of the message and Destination is the intended destination of the message irrespective of a potential relay function between the transaction endpoints.
  - Transaction ID for the first transaction for tuple {Source, Destination, MSID, Function Type, R6\_Context\_ID} SHALL be set to random non-zero value where R6\_Context\_ID SHALL be taken into account if present.
  - 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 or Indication-Ack 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, R6\_Context\_ID} where R6\_Context\_ID SHALL be taken into account if present, 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 may be set by the sender in any message which initiates a new transaction (except for 1-way transactions), when the re-synchronization of Transaction ID is required. “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, R6\_Context\_ID}, where R6\_Context\_ID SHALL be taken into account if present, 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, R6\_Context\_ID}, where R6\_Context\_ID SHALL be taken into account if present, 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, R6\_Context\_ID}, where R6\_Context\_ID SHALL be taken into account if present, 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:
    - This is the first transaction for the specified function type after MS (identified by MSID in the header, and R6\_Context\_ID if present) state change from Active to Idle.
    - This is the first transaction for the specified function type after MS (identified by MSID in the header, and R6\_Context\_ID if present) 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.
    - This is the first transaction for the specified function type after new MS (identified by MSID in the header, and R6\_Context\_ID if present) 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, R6\_Context\_ID}, where R6\_Context\_ID SHALL be taken into account if present, 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  $T_{\text{missing}}$  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 transaction is received before the timer expiration, or any transaction with “R” bit is received for the same tuple {Source, Destination, MSID, Function Type, R6\_Context\_ID} where R6\_Context\_ID SHALL be taken into account if present. When the timer  $T_{\text{missing}}$  expires, corresponding missing transaction is declared lost and the receiver SHALL discard any subsequent messages associated with that transaction.
  - Reserved: Bits SHALL be set to 0 by the sender; the receiver SHALL ignore all bits.
  - Destination Identifier TLV: Variable-length identifier of the Destination Entity, as defined in [1]; i.e., ID of the Network Node which hosts the Functional Entity which is the intended destination of the message body.
- Receiver of the message should check Destination Identifier TLV in the header. If Destination Identifier indicates the receiver's Identifier, receiver should process the message. Otherwise receiver should relay the message to Destination Identifier without any change.
- Source Identifier TLV: Variable-length identifier of the Source Entity, as defined in [1]; i.e., ID of the Network Node which hosts the Functional Entity that is the originator of the message body.
  - R6\_Context\_ID TLV: If present, it SHALL be the first TLV following the Source Identifier and Destination Identifier TLVs if these are present or it SHALL be the first TLV following the message header if the Source Identifier and Destination Identifier TLVs are not present, as shown in Figure 3-2. The receiver of the message SHALL always check whether the R6\_Context\_ID is present.

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

### 3.2.1 Usage of Source Identifier and Destination Identifier TLV

ASN control protocol messages are exchanged between peer entities. In specific cases described below an intermediate node of the ASN is used to relay messages between the peer entities.

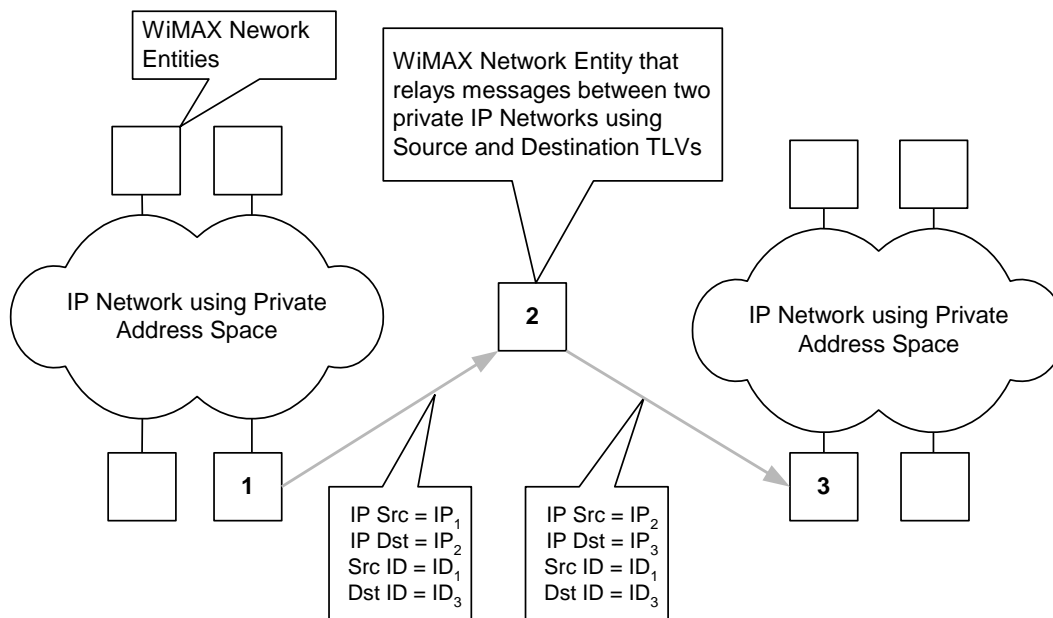
This is done by using the Relay mode of operation:

In the Relay mode of operation:

- the Source Identifier and Destination Identifier TLVs identify the logical entities associated with the processing of the messages;
- the Source Identifier and Destination Identifier TLVs SHALL be the first TLVs in the message as shown in Figure 3-2;
- the T bit SHALL be set to 1.

Source Identifier and Destination Identifier TLVs SHALL be included if Destination Identifier value is not equal to the destination IP address.

The Source and Destination Identifier TLVs are used to allow message delivery between WiMAX Entities that do not have direct IP connectivity between them. Figure 3-4 gives an example of the ASN separated into two IP Clouds each of which uses Private IP Address space. IP messages within each cloud are delivered using IP routing mechanisms. However the messages between the clouds cannot rely on IP routing. Instead the WiMAX Entities located on the border between the clouds relay the messages using Source and Destination Identifier TLVs.



**Figure 3-4 – Example of ASN Separated into Two Private IP Clouds**

A WiMAX Entity, which relays messages based on Source and Destination ID TLVs, SHALL be capable of translating every ID into the corresponding IP Address within each IP routable cloud connected to this entity. This translation is shown on Figure 3-4, which shows Entity 1 sending a message to Entity 3 via Entity 2.

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

Mapping IDs onto IP Addresses is an implementation issue.

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

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

### 3.2.2 Transport Protocol Usage

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

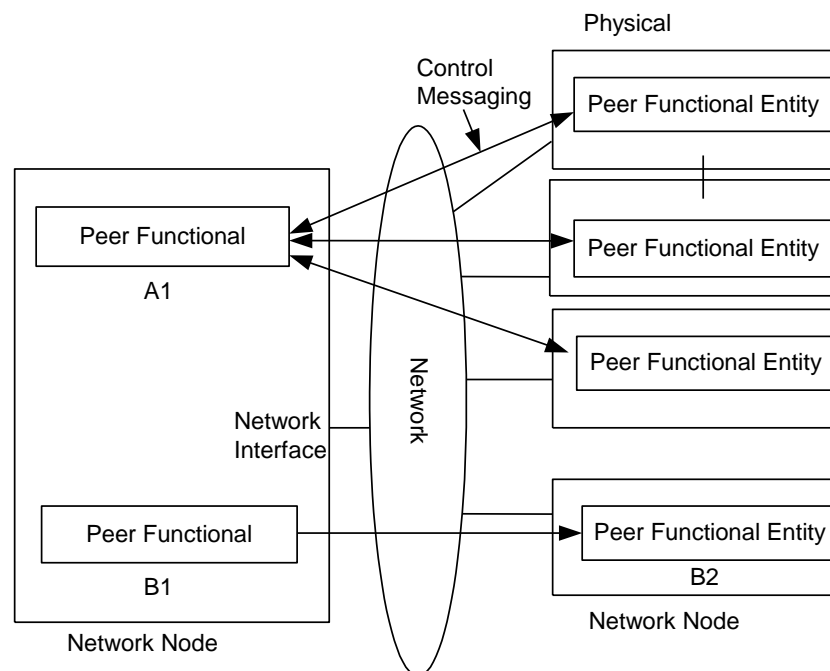
UDP checksum is mandatory when used with IPv4.

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

### 3.3 Transport Protocol

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

Figure 3-5 illustrates the essential aspects of control messaging between functional entities. Here, communication between peer elements of two functional entities A and B are shown. Each peer entity is realized in a Network Node (e.g., a BS), which has connectivity to an L2 or L3 network. The figure shows that whereas peer functional entities A and B are collocated in the same physical implementation on one side, they are located in different implementations on the other side. The figure also shows communication between peer functional entities. Whereas functional entity A1 on the left communicates with more than one peer on the right, functional entity B1 on the left communicates with the single peer B2 on the right. For the peer entities to communicate there SHALL be a path between the corresponding physical implementations, for instance, direct IP connectivity or a tunnel.



**Figure 3-5 – Communication Model**

UDP/IP SHALL be used as the transport protocol for communication between peer functional entities. The peer functional entity (FE) at each end is addressed by the ID of the Network Component which hosts the FE, in combination with the Function Type (e.g., QoS, HO, R3MM) which is part of the WiMAX NWG Message Header

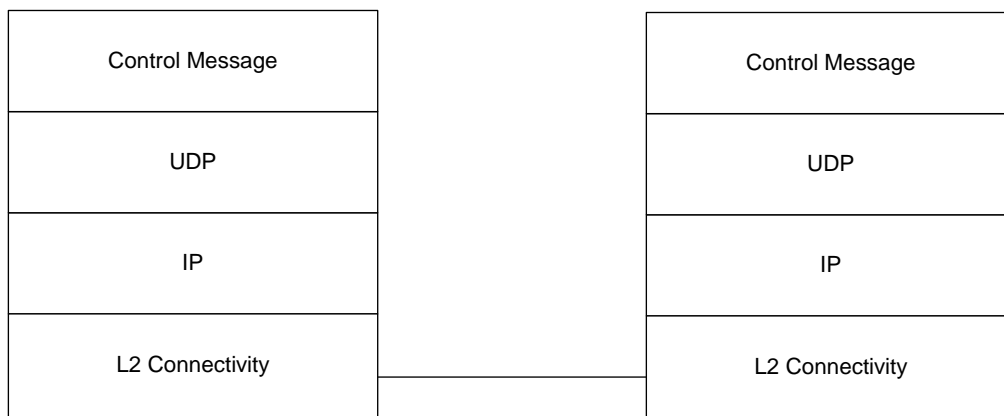
(section 3.2). The list of Function Types is given in Table 5-1. This IP address SHALL be one of the IP addresses assigned to the corresponding physical implementation. The UDP/IP messages between peer entities MAY be tunneled between the corresponding physical implementations, but this is transparent to the functional entities.

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

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

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

The protocol stack representation for control message communication is shown in Figure 3-6. The L2/L3 connectivity represents the communication path between the functional entities. The IP layer packets between the functional entities will be encapsulated in specific manner depending on the nature of the connectivity (for instance, GRE encapsulation for GRE tunnels). The outer envelope of the encapsulated packet would then have addressing information that enables the intervening L2/L3 network to deliver the packet to the appropriate physical implementation.



**Figure 3-6 – Protocol Layers**

## **3.4 Transport Requirements**

### **3.4.1 Reliable Message Delivery**

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

### **3.4.2 Message Size and Fragmentation**

The size of a UDP message is limited to 65535 bytes. The size of messages between functional entities SHALL therefore be less than this. Larger messages SHALL be fragmented at the application. As the size of UDP messages MAY be limited by the path MTU size, fragmentation as defined by [20] & [21] SHALL be supported.

### **3.4.3 ASN Bearer Plane MTU Size**

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



## 3.5 Error Handling and handling of unknown and inopportune control information

This section specifies

- the handling of erroneous, unknown and inopportune control information by the receiver (section 3.5.1);
- the reporting of an error to the sender (section 3.5.2);
- the reaction on receipt of an error report (section 3.5.3);
- the handling of internal errors (section 3.5.4).

### 3.5.1 Handling of erroneous, unknown and inopportune control information by the receiver

Erroneous control information will be received due to transmission errors.

Unknown control information will be received due to transmission errors (this is an error case), but also because new control information has been specified in the evolution of the protocol.

Inopportune control information, i.e., control information that is not consistent with the state of the receiver or with the context (e.g., a known TLV in a message where the TLV is not defined or foreseen) will be diagnosed by the receiver in certain cases when there was an internal error or a transmission error, but also because new usage of known control information has been specified in the evolution of the protocol.

This section specifies the general behavior of the receiver when erroneous, unknown or inopportune control information has been received; specific requirements of other sections within this specification take precedence over this section.

The general reaction of the receiver when erroneous, unknown or inopportune control information has been received is:

- to diagnose an error, possibly with additional attributes; for example the error may indicate 'Message Header Failure' and the attribute may indicate 'Destination unknown';
- if required to report the error;
- as required either skip the information or reject it.

#### 3.5.1.1 Initial actions on an incoming control message

This section specifies the sequence of initial actions to be performed by the receiver of a message.

When a message is received and parsing of the message header is not successful, the receiver SHALL diagnose a 'Message Header Failure' error with attribute 'Invalid Message Header' and report it to the sender.

Otherwise, if the T bit indicates presence of the Destination Identifier TLV and Source Identifier TLV in the message, the receiver SHALL check the conditions in the table below one after the other until the first error is diagnosed or until all conditions have been checked without an error having been diagnosed. If and when a first condition is found to be fulfilled,

the receiver SHALL diagnose a 'Message Header Failure' error with attribute as indicated in the table;

the receiver SHALL report the error to the sender using the Error Reflection method as specified in section 3.5.2;

the receiver SHALL otherwise skip the message.

Step	Condition	Attribute of error diagnosed
A	Destination Identifier TLV is not present as first TLV in the message	'Destination Identifier missing or erroneous'
B	Destination Identifier TLV is erroneous	'Destination Identifier missing or erroneous'

C	Destination in Destination Identifier TLV is unknown	'Destination unknown'
D	Source Identifier TLV is not present as second TLV in the message as second TLV	'Source Identifier TLV missing or erroneous'
E	Source Identifier TLV is erroneous	'Source Identifier TLV missing or erroneous'
F	Source Identifier TLV is inconsistent with the IP source address	'Source Identifier unknown or inconsistent with the IP source address'

Otherwise if the Destination Identifier TLV is present in the message and the receiver is not the destination, the receiver SHALL proceed as specified in section 3.2.1 without further interpreting the message.

Otherwise, if the R6\_Context\_ID TLV is present in the message, the receiver SHALL check the conditions in the table below one after the other until the first error is diagnosed or until all conditions have been checked without an error having been diagnosed. If and when a first condition is found to be fulfilled,

the receiver SHALL diagnose a 'Message Header Failure' error with attribute as indicated in the table;

the receiver SHALL report the error to the sender using the Error Reflection method as specified in section 3.5.2;

the receiver SHALL otherwise skip the message.

Step	Condition	Attribute of error diagnosed
A	R6_Context_ID TLV is not present as first TLV in the message, after the Destination Identifier and Source Identifier TLVs if these are present.	'R6_Context_ID missing or erroneous'
B	R6_Context_ID TLV is erroneous	' R6_Context_ID missing or erroneous'

Otherwise, if the message is an Error Reflection message (see section 3.5.2), the receiver SHALL proceed as specified in section 3.5.3.

Otherwise, if the Function type is unknown:

- if comprehension is required for the Function type, the receiver SHALL report a 'Message Header Failure' error with attribute 'Unrecognized Function Type' to the sender, using the error reporting as explained in 3.4.3
- if comprehension is not required for the Function type, the receiver SHALL not report a corresponding error to the sender.

In both cases the receiver SHALL not take any further protocol related action on the message unless otherwise required by this specification.

Otherwise, if another message with matching TID is being processed, the receiver SHALL discard the latter message.

Otherwise, if the message indicates TID = X but TID > X was expected, the receiver SHALL discard the latter message.

Otherwise, the receiver SHALL process the Transaction ID as specified in section 3.2; then if the Message type is unknown or inopportune:

- if comprehension is required for the message type, the receiver SHALL report a 'Message Header Failure' error with attribute 'Message type unknown or inopportune' to the sender;

– if comprehension is not required for the message type, the receiver SHALL not report a corresponding error to the sender.

In both cases the receiver SHALL not take any further action on the message unless otherwise required by this specification.

Otherwise, if the receiver discovers an error in the message header, the receiver SHALL:

- if a specific handling is required by other parts of this specification, perform this handling;
- if a specific handling is not required by other parts of this specification, diagnose a 'Message Header Failure' error with attribute 'Unresolved error' and report it.

Otherwise, the receiver SHALL process the header as required by the protocol.

After processing the header, the receiver SHALL process the remaining TLVs as specified below; if the receiver diagnoses an error while processing the remaining TLVs as specified below, the error is known to have occurred on a level below the message type.

### 3.5.1.2 Subsequent error diagnostics

After the actions of section 3.5.1.1, the remaining TLVs SHALL be processed.

Table 3-1 captures the default processing of the remaining TLVs in an ASN control message. It applies if other parts of this specification do not require different processing. The default processing applies to all TLVs including nested TLVs.

The order of processing TLVs is an implementation matter with the following restriction:

- Before a nested TLV is processed, the receiver SHALL have processed Type and length of the parent TLV.

Note: Examples of order of processing are 'depth first' and 'breadth first'.

If the protocol does not require the receiver to process a TLV, the receiver MAY skip the TLV without carrying out any error diagnostics except for the TLV parsing error.

Note: The preferred way is the sender to set 'TLV comprehension not required' (TC = 1) in the case described above. This rule was introduced in order to deal with transition problems, in particular to allow the same TLV coding when a TLV is sent to legacy and non-legacy nodes. It should be revisited in later versions.

**Table 3-1 – Processing of TLVs, Abnormal Cases**

Abnormal Case	Explanation	Action
Unknown TLV	The Type of the TLV is not known in the message or in the parent TLV.	The receiver SHALL diagnose a 'General Message Body Failure' error with attribute 'TLV unknown' and proceed as specified in section 3.5.1.3.
Mandatory TLV not included	The message definition resp. TLV definition specifies presence of a TLV with the indicated Type as 'M'; no TLV with the indicated Type is present in the message resp. TLV.	The receiver SHALL diagnose a 'General Message Body Failure' error with attribute 'mandatory TLV missing' and report the error to the sender as specified in section 3.5.2.
Unforeseen TLV repetitions	The message definition resp. TLV definition specifies a TLV with the indicated <i>Type</i> value; more TLV with the indicated	The receiver SHALL use the first TLV occurrences up to the specified number; then - if for at least one further occurrence of the TLV in the message, TLV

	<i>Type</i> value are present in the message resp. TLV than specified in the message definition resp. TLV definition.	comprehension is required, the receiver SHALL <ul style="list-style-type: none"> <li>○ diagnose error 'General Message Body Failure' error with attribute "TLV unexpected";</li> <li>○ and proceed as specified in section 3.5.1.3;</li> <li>○ the position of the error is the position of the first further occurrence of the TLV in the message requiring comprehension;</li> </ul> - otherwise the receiver SHALL skip the remaining occurrences of the TLV.
TLV parsing error	e.g.: <ul style="list-style-type: none"> <li>- the message is too short to contain the Length field of the TLV;</li> <li>- the message is too short to contain a TLV with indicated length;</li> <li>- or, the TLV is too short to contain all required fields.</li> </ul>	The receiver SHALL diagnose error 'General Message Body Failure' with attribute 'TLV parsing error', report an error to the sender and otherwise skip the message.
TLV too long	After parsing the TLV, further bytes remain (as indicated by the Length field).	The receiver SHALL skip the remaining bytes of the TLV.
Reserved value	A field in the TLV contains a reserved value.	The receiver SHALL diagnose error 'General Message Body Failure' with attribute 'TLV Value Invalid' and proceed as specified in section 3.5.1.3.

For the definition of 'TLV comprehension required', see section 5.3.1.

### 3.5.1.3 Actions when an error has been diagnosed

In this section, the following definitions are used:

A TLV (TLV1) is an *ancestor of* another TLV (TLV2) if

TLV1 is the parent TLV of TLV2 or

TLV1 is the parent TLV of a third TLV (TLV3) that is ancestor of TLV2.

A TLV is known to *surround an error* (error as described in the previous section) if

the error was diagnosed in a field of the TLV; or

the error consists in the Type of the TLV being not known in the message or in the parent TLV;

the error occurred because the TLV is an unforeseen repetition; or

the error occurred in the Value part of the TLV; or

the TLV is parent TLV of a TLV surrounding the error.

A TLV is *the closest skipable TLV to an error* if

the TLV surrounds the error; and

the TLV indicates 'comprehension not required' as specified in section 5.3.1; and  
the TLV does not surround another TLV surrounding the error and indicating 'comprehension not required'.  
The general error handling specified in this section is as follows:  
Unless otherwise specified, the receiver SHALL:  
if it exists, skip the closest skipable TLV to the error and continue processing the message;  
if there is no closest skipable TLV to the error, report an error to the sender of the message and otherwise skip the message.

#### 3.5.1.4 Subsequent handling of abnormal cases in the message flow of transactions

Table 3-2 specifies subsequent handling of abnormal cases in the message flow of transactions:

**Table 3-2 – Handling of Message Flow of Transactions, Abnormal Cases**

Abnormal Case	Explanation	Action
No response received from peer after sending Request/Response message		Retransmit until max retries exhausted.
Out of order message, skipped TID	TID = Y > X received when the next expected TID = X	Process the message normally. The receiver starts timer $T_{\text{missing}}$ awaiting the missing transaction.
Request to terminate or delete context or datapath that does not exist		Send response with Success or other code to prevent repeated requests Move to specific parts

After a message is processed successfully at the receiver, a “success” indication to the sender is implicit in the reply generated to the message received .e.g., a *Path\_Reg\_Rsp* in reply to *Path\_Reg\_Req* etc.

#### 3.5.2 Error reporting

There are two methods for the receiver of a message to report an error to the sender:

- the Error Response method and
- the Error Reflection method.

1. **Error Response method:** Unless otherwise specified, the receiver of a message SHALL use this method to report an error to the sender if both conditions (a) and (b) apply:

(a) the error occurred on a level below the message type (for the definition of the term 'level below the message type'. see section 3.5.1.1, action 0);

(b) one of conditions (b1) and (b2) applies:

(b1) the erroneous message is a REQ message for which an RSP message is specified;

(b2) the erroneous message is an RSP message for which an ACK message is specified.

In order to use the Error Response method the receiver SHALL send back to the sender an Error Response message. The Error Response message is:

- in case (b1) an RSP message corresponding to the erroneous message;
- in case (b2) an ACK message corresponding to the erroneous message.

The Error Response message SHALL contain a Failure Indication TLV at the *first free position after the header* (see below), optionally immediately followed by a Failure Indication Details TLV.

2. **Error Reflection method:** The receiver of a message SHALL use this method to report an error to the sender if the Error Response method does not apply.

In order to use the Error Reflection method the receiver SHALL send back to the sender an Error Reflection message. The Error Reflection message is a copy of the received erroneous message, with the following modifications:

- the E bit is set to 1;
- the T bit is set to 1 if the Relay Mode of operation is used to transfer the Error Reflection message; the T bit is set to 0 if the Relay Mode of operation is not used to transfer the Error Reflection message;
- a Failure Indication TLV is included at the *first free position after the header* (see below), optionally immediately followed by a Failure Indication Details TLV;
- the Error Reflection message MAY, as an option, omit all top-level TLVs (including their full Value part; in particular including all nested TLVs) following the reported error; this means:
  - o if the reported error occurred on a level below the message type (for the definition of the term 'level below the message type' see section 3.5.1.1, action 0), omit all top-level TLVs of the erroneous message following the top-level TLV surrounding the error;
  - o otherwise, omit all top-level TLVs that are neither the Destination Identifier TLV nor the Source Identifier TLV;
- the value of the Length field of the message is adjusted.

The *first free position after the header* is:

- the position immediately following the header if both the T bit is set to 0 and no R6\_Context\_ID TLV is present;
- otherwise, the position after the (first) occurrence of the Source ID if no R6\_Context\_ID TLV is present;
- otherwise, the position after the (first) occurrence of the R6\_Context TLV.

Note: as a consequence, in the cases of section 3.5.1.1, action 0 conditions b or c are met, the Destination ID of the erroneous message will be contained in the Error Reflection message after the Failure Indication TLV (and possibly the Failure Indication Details TLV).

In both methods, the Failure Indication TLV and the Failure Indication Details TLV (if included) SHALL take appropriate values resulting from the error diagnosis.

### 3.5.3 Reaction on receipt of an error report

When an R4/R6/R8 entity receives an error message, that is an Error Reflection message or an Error Response message, it SHALL check whether the error message is syntactically and semantically correct. If it is not correct, the receiver:

- MAY try to understand the error message and proceed with that understanding; or
- MAY ignore the error message.

Detailed reaction on receipt of an error report is implementation dependent, however the following recommendations are given:

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

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

1 If the Source and Destination TLVs are present, the Failure Indication TLV should be the first TLV included after  
2 these TLVs.

3 In the case of a 3-way transaction, the R6/R4 peer should abort the current transaction upon the receipt of a response  
4 message with Failure Indication TLV and should not send an Acknowledge message. Also, upon receiving a bad  
5 Response message (in a 3-way transaction), an Acknowledge message should be sent with Failure Indication TLV.  
6 In both these cases, the peer receiving the Failure Indication TLV may follow with one of the following actions:

- 7 A. In general, the peer may retransmit the earlier R6/R4 message.
- 8 B. The peer can abort the current transaction and may start a new independent transaction. This new  
9 transaction may or may not be network exit procedures.
- 10 C. The peer can proceed to run network exit procedures.

11 When an R6/R4 peer receives a message corresponding to an ‘old’ transaction, one of the following actions may be  
12 taken:

- 13 A. If an ‘old’ Acknowledgement message is received in the case of a 3-way transaction, it can be ignored.
- 14 B. Last message in every 2-way (e.g., Response) and 3-way transaction (e.g., Acknowledgement) should  
15 be kept to accommodate the loss of this last message. If the peer retransmits the previous message, the  
16 saved last message should be re-sent without any modification in its original content.
- 17 C. In all other cases, the out of order message should be discarded.

#### 18 **3.5.4 Asynchronous Error Indication to Peers**

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

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

---

## 4. Control Plane Protocols and Procedures

This section describes the WiMAX network control plane protocols and procedures.

When two ASN instances are co-located, the call flow interactions between the two ASN instances are not specified.

For all messages specified, with the exception of Source Identifier, Destination Identifier, and R6\_Context\_ID TLVs ordering of mandatory and optional TLVs are not enforced by the sender or receiver. Any timers that have not been specified in this release with default, minimum and maximum values will be specified in a future revision or release of this specification.

Messages or attributes requiring an Enterprise number or Vendor ID in this release uses 24757 as assigned by IANA for the WiMAX Forum.

NOTE-1: The ASN Architecture is functionally decomposed based on what used to be known as ASN Profile C in NWG Release 1.0

NOTE-2: An ASN may be implemented in a fashion that only exposes external reference points R1, R3, and R4 and doesn't expose R6 and R8. One example of this implementation is an ASN comprised of a single physical element (e.g. Integrated BS/GW) supporting the BS and ASN-GW functions.

### 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

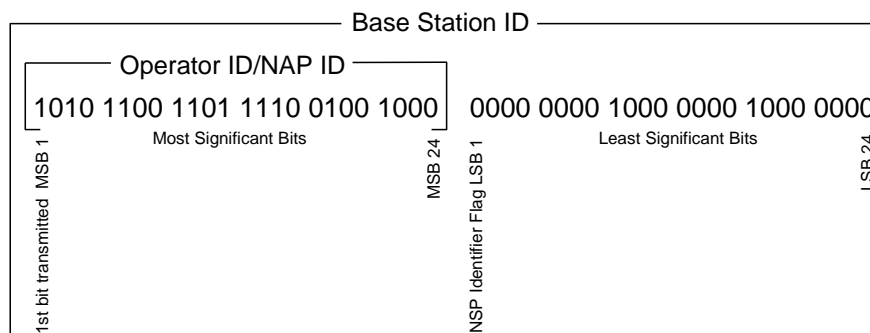
An MS detects available NAP(s) by scanning and decoding DL-MAP of ASN(s) on detected channel(s). The most significant 24 bits (MSB 24 bits) of the "Base Station ID" SHALL be used as Operator ID, which is the NAP Identifier. NAP discovery is based on the procedures defined in IEEE Std 802.16 [10] and 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 Plans and CAPL is available in configuration information, it MAY be used to improve efficiency of NAP discovery (See Section 4.1.3 for further information).

##### 4.1.2.2 NSP Discovery

The NAP MAY support more than one NSP. Also, the NAP SHALL present separate NSP identifier(s), 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 and verbose NSP names presented over the air interface as part of SII-ADV and/or SBC-RSP and all NSP realms that can be obtained using SBC-REQ/RSP SHALL be uniform across all Base Stations of the same NAP ID. Also, the NSP change count in DCD 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. However, MS MAY request NSP identifiers even though NSP Identifier Flag is set to a value of '0' and the BS SHALL respond with the requested NSP identifiers.



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

In the NAP+NSP deployment case where there is only one NSP associated with the NAP and where no regulatory or deployment reasons compel separate presentation of an NSP identifier, the NAP SHALL set NSP Identifier Flag to a value of '0'. In this case, when the MS detects the identifier of a NAP, the MS knows the identifier of associated NSP. The MS MAY continue NSP discovery to obtain verbose NSP name of the NSP.

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

**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	3FFFFFF	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	FFFFFF	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	11111111001111111100111	FF9FE7	16752615	
First public OID	11111111001111111101000	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	

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

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

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

The MS SHALL sequentially perform NSP Discovery with each NAP for the purpose of discovering the supported NSPs. If reported MS MAC Version Number is equal to 6 (i.e. sent in TLV-148 of the *RNG-REQ* message), the NAP SHALL connect the MS to a default NSP i.e. pre-configured in the ASN-GW. The list of available NAPs MAY be further categorized as 'User Controlled CAPL' and/or 'Operator Controlled CAPL' (categorization and prioritization of 'User Controlled CAPL' based on NAP ID lists is a deployment detail and beyond the scope of this specification). If such categories of lists are available, selection MAY proceed as follows:

- If the "User Controlled CAPL" is available in the MS, each NAP in the "User Controlled CAPL" in the MS (in priority order):
  - if the identifier(s) of NSP(s) supported by the NAP is available in the configuration information stored in the MS and the value of the NSP Change Count TLV sent in the DCD message from networks is equal to the value of NSP Change Count stored in the SS, then the supported NSPs and Verbose NSP Names SHOULD be enumerated locally and the identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of available NSPs".
  - if the identifier(s) of NSP(s) supported by the NAP is NOT available in the configuration information stored in the MS, or if the value of the NSP Change Count TLV sent in the DCD message from networks is NOT equal to the value of NSP Change Count stored in the MS, then the MS SHALL obtain the identifier(s) of supported NSP(s) through receiving NSP List TLV and Verbose NSP Name List TLV. NSP List TLV and Verbose NSP Name List TLV may be obtained either through unsolicited, periodic BS transmittal of an SII-ADV broadcast message, or the MS may transmit SBC-REQ message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS transmittal of NSP List TLV, or the MS may transmit SBC-REQ message including SIQ TLV with 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 NSP List TLV and Verbose NSP Name List TLV. The network SHALL respond with the requested NSP identifier(s) either through an SII-ADV broadcast or SBC-RSP unicast transmission. The identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of available NSPs". After obtaining and storing the identifiers of supported NSPs, the MS SHALL restart the ND&S process.
- If the "Operator Controlled CAPL" is available in the MS, each NAP in the "Operator Controlled CAPL" in the MS (in priority order):
  - if the identifier(s) of NSP(s) supported by the NAP is available in the configuration information stored in the MS and the value of the NSP Change Count TLV sent in the DCD message from networks is

<sup>1</sup> 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@ieee.org](mailto:IEEE.Registration.Authority@ieee.org).

<sup>2</sup> 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>

equal to the value of NSP Change Count stored in the SS, then the supported NSPs and Verbose NSP Names SHOULD be enumerated locally and the identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of available NSPs".

- if the identifier(s) of NSP(s) supported by the NAP is NOT available in the configuration information stored in the MS, or if the value of the NSP Change Count TLV sent in the DCD message from networks is NOT equal to the value of NSP Change Count stored in the MS, then the MS SHALL obtain the identifier(s) of supported NSP(s) through receiving NSP List TLV and Verbose NSP Name List TLV. NSP List TLV and Verbose NSP Name List TLV may be obtained either through unsolicited, periodic BS transmittal of an SII-ADV broadcast message, or the MS may transmit SBC-REQ message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS transmittal of NSP List TLV, or the MS may transmit SBC-REQ message including SIQ TLV with 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 NSP List TLV and Verbose NSP Name List TLV. The network SHALL respond with the requested NSP identifier(s) either through an SII-ADV broadcast or SBC-RSP unicast transmission. The identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of available NSPs". After obtaining and storing the identifiers of supported NSPs, the SS SHALL restart the ND&S process.
- If neither "User Controlled CAPL" nor "Operator Controlled CAPL" is available in the MS, each NAP in implementation specific order:
  - if the identifier(s) of NSP(s) supported by the NAP is available in the configuration information stored in the MS and the value of the NSP Change Count TLV sent in the DCD message from networks is equal to the value of NSP Change Count stored in the MS, then the supported NSPs and Verbose NSP Names SHOULD be enumerated locally and the identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of available NSPs".
  - if the identifier(s) of NSP(s) supported by the NAP is NOT available in the configuration information stored in the MS, or if the value of the NSP Change Count TLV sent in the DCD message from networks is NOT equal to the value of NSP Change Count stored in the MS, then the MS SHALL obtain the identifier(s) of supported NSP(s) through receiving NSP List TLV and Verbose NSP Name List TLV. NSP List TLV and Verbose NSP Name List TLV may be obtained either through unsolicited, periodic BS transmittal of an SII-ADV broadcast message, or the MS may transmit SBC-REQ message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS transmittal of NSP List TLV, or the MS may transmit SBC-REQ message including SIQ TLV with 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 NSP List TLV and Verbose NSP Name List TLV. The network SHALL respond with the requested NSP identifier(s) either through an SII-ADV broadcast or SBC-RSP unicast transmission. The identifiers of supported NSPs, including Verbose NSP Names, SHALL be added to the "list of available NSPs". After obtaining and storing the identifiers of supported NSPs, the SS SHALL restart the ND&S process.

The "list of available NSPs" is processed to highlight the available and allowed NSPs. The NSPs which have been barred through the Network Rejection procedure (see sub-clause 4.5.1.3) are not included in this list.

The encoding of the verbose NSP name SHALL be UTF-8 whenever transferred over R1 interface.

When SBC-REQ/RSP procedure is used for ND&S procedure, BS doesn't continue the PKM procedure for the given MS after SBC-RSP is sent. In other words, BS doesn't send MS\_PreAttachment\_Req to ASN-GW if SBC-REQ has SIQ TLV.

If a MS chooses to perform network entry at a BS, it SHALL NOT include the SIQ TLV in its SBC-REQ. When MS does not include the SIQ TLV in its SBC-REQ, the BS SHALL continue the PKM procedure for the given MS after SBC-RSP is sent.

#### 4.1.2.3 NSP Enumeration and Selection

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

The MS SHALL produce a list of available NSPs as discovered through NSP Discovery in the available NAPs, as identified in NAP Discovery. The MS SHALL NOT allow selection of an NSP that has been barred through the Network Rejection Procedure (see sub-clause 4.5.1.3) if the conditions imposed by the rejection procedure on future access attempts have not been met. The NSP Enumeration List is used for both manual and automatic selection.

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

#### **4.1.2.3.1 Manual Mode**

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

- a. Home NSP.
- b. If the "User Controlled RAPL" is available, NSPs or their corresponding Verbose NSP Names in the "User Controlled RAPL" in the MS (in priority order).
- c. If the "Operator Controlled RAPL" is available, NSPs or their corresponding Verbose NSP Names in the "Operator Controlled RAPL" in the MS (in priority order).
- d. Any other NSP or their corresponding Verbose NSP Names in random order.

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

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

#### **4.1.2.3.2 Automatic Mode**

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

The MS SHALL select and attempt to authenticate with an available and allowable (according to configuration information defined in Section 4.1.3) NSP, in the following precedence:

- a. Home NSP.
- b. If the "User Controlled RAPL" is available, NSPs in the "User Controlled RAPL" in the MS (in priority order).
- c. If the "Operator Controlled RAPL" is available, NSPs in the "Operator Controlled RAPL" in the MS (in priority order).
- d. Any other NSP in random order.

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

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

#### **4.1.2.4 ASN Attachment**

Following a decision to select an NSP, an MS indicates its NSP selection by attaching to an ASN associated with the selected NSP, and by providing its identity and home NSP domain in form of NAI (see Section 4.4.1.3). The ASN uses the realm portion of the NAI to route AAA transactions for the MS. When the NSP Identifier Flag is set to a value of "1", i.e., NAP-Sharing, the MS SHALL use its NAI with additional information when presented (also known as decorated NAI described in IETF [68]) to influence the routing choice of the next AAA hop when the home NSP realm is only reachable via another mediating realm (e.g., a visited NSP). However, in the NAP+NSP case where the NSP Identifier Flag is set to a value of "0", the MS MAY NOT decorate the realm portion of NAI

with the visited NSP realm. The MS is expected to use same NAI decoration that was used in initial entry for all subsequent re-authentications.

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

If the MS does not have the realm of a visited NSP stored in the configuration information such that the MS can construct a properly formatted EAP Information Request with appropriate routing decoration to influence the routing choice of the next AAA hop, then the MS MAY include the Visited NSP ID TLV in the SBC-REQ message to solicit BS transmittal of the Visited NSP Realm TLV in the SBC-RSP message, as specified in Std IEEE 802.16. If included, the format of the realm within Visited NSP Realm TLV SHALL be as specified in [68].

Note: realm change during reauthentication compared to realm used in initial network entry will result in an Access-Reject from the AAA, or a hotline to a dedicated server based on an operator's policy.

### 4.1.3 Configuration Information

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

Configuration information SHOULD include items as follows:

User/Operator Controlled CAPL

User/Operator Controlled CAPL contain the Network Access Providers, who have direct relationship with the Home Network Service Provider. If a selected NSP MAY be reached through more than one NAP, the list is used to select a NAP in the case of automatic NSP Enumeration and Selection phase.

The user controlled CAPL has higher priority than the Operator Controlled CAPL.

CAPL SHALL contain NAP ID and MAY contain Priority for each NAP.

NAP Selection Policy MAY be included into CAPL. The NAP Selection Policy applies only to the User or Operator Controlled CAPL it is associated to. Table 4-2 defines the possible values for NAP Selection Policy.

**Table 4-2 – NAP Selection Policy Values in CAPL**

NAP Selection Policy	Description
Strict Policy	Device SHALL not establish connection to the H-NSP using NAPs which are not in CAPL. Device SHALL NOT select a forbidden NAP to establish connection to the H-NSP.
Partially Flexible Policy	Device SHALL establish connection to the H-NSP using NAPs which are in CAPL before selecting a NAP which is not in CAPL. NAPs in CAPL have higher priority than NAPs which are not in CAPL. Device SHALL NOT select a forbidden NAP to establish connection to the H-NSP.
Fully Flexible Policy	Device is allowed to establish connection to the H-NSP using any NAP. The NAPs in CAPL which do not include a priority are considered to have the same priority as the NAPs which are not in the CAPL. Device SHALL NOT select a forbidden NAP to establish connection to the H-NSP.

Priority MAY be assigned to each NAP in CAPL to make preferences between different NAPs compared to the other ones. If the priority is not assigned to a NAP and NAP Selection Policy is Fully Flexible Policy, the NAP does not have any priority over other NAPs. If priority is not assigned to a NAP and NAP Selection Policy is Partially Flexible Policy, NAPs in CAPL still have higher priority than NAPs which are not in CAPL. The device MAY ignore the priorities of NAPs if no preferred NAPs are found with NAP discovery based on Root Channel Plan and the value of NAP Selection Policy node equals to Partially Flexible Policy or Fully Flexible

Policy. It is recommended to define Priority when selecting of a more preferred NAP is important. Having different priorities without NAP based or Root Channel Plan causes significant implication on the NAP discovery time. The highest priority NAP SHALL be selected from the available NSPs.

CAPL MAY also contain forbidden NAPs through which the MS is not allowed to establish connection to the H-NSP.

List of one or more Channel Plans can be associated to a NAP in CAPL to create NAP Based Channel Plan for each NAP (see Channel Plan for more information about NAP Based Channel Plan).

User/Operator controlled NSP Identifier list.

User/Operator Controlled RAPL contain the Visited Network Service Providers, who have direct relationship with the Home Network Service Provider. In the case of automatic NSP Enumeration and Selection mode, the lists are used to select a NSP with highest priority for roaming when NAPs, which have direct connection to the H-NSP, are not available. In the case of manual NSP Enumeration and Selection mode, the lists are used to determine the order of presenting available NSPs to a user. The user controlled RAPL has higher priority than the Operator Controlled RAPL.

RAPL SHALL contain V-NSP ID and MAY contain Priority for each V-NSP.

V-NSP Selection Policy MAY be included into RAPL. The V-NSP Selection Policy applies only to the User or Operator Controlled RAPL it is associated to. Table 4-3 defines the possible values for V-NSP Selection Policy.

**Table 4-3 – V-NSP Selection Policy Values in RAPL**

V-NSP Selection Policy	Description
Strict Policy	Device SHALL not establish connection to the H-NSP using V-NSPs which are not in RAPL. Device SHALL NOT select a forbidden V-NSP to establish connection to the H-NSP.
Partially Flexible Policy	Device SHALL establish connection to the H-NSP using V-NSPs which are in RAPL before selecting a V-NSP which is not in RAPL. V-NSPs in RAPL have higher priority than V-NSPs which are not in RAPL. Device SHALL NOT select a forbidden V-NSP to establish connection to the H-NSP.
Fully Flexible Policy	Device is allowed to establish connection to the H-NSP using any V-NSP. The V-NSPs in RAPL which do not include a priority are considered to have the same priority as the V-NSPs which are not in the RAPL. Device SHALL NOT select a forbidden V-NSP to establish connection to the H-NSP.

Priority MAY be assigned to each V-NSP in RAPL to make preferences between different V-NSPs compared to the other ones. If the priority is not assigned to a V-NSP and V-NSP Selection Policy is Fully Flexible Policy, V-NSP does not have any priority over other V-NSPs in NSP selection. If priority is not assigned to a V-NSP and V-NSP Selection Policy is Partially Flexible Policy, V-NSPs in RAPL still have higher priority than V-NSPs which are not in RAPL.

RAPL MAY also contain forbidden V-NSPs through which the MS is not allowed to establish connection to the H-NSP.

NAP/NSP Mapping List.

NAP/NSP Mapping List indicates the supported NSPs, with corresponding Verbose NSP Names, per NAP.

NSP Change Count.

NSP Change Count indicates whether the list of supported NSPs or Verbose NSP Names for a NAP is changed.

NSP Realm

Mapping table between 24-bit NSP identifiers and corresponding realm of the NSPs.

Channel Plan

Channel Plan contains physical information: Information useful in NAP Discovery including channel, center frequency, and PHY profiles.

The primary motivation behind providing the Channel Plan information to the device is to speed up the network discovery and selection process. The Channel Plan MAY cover physical information of multiple or all NAPs, which are listed in CAPL. The Channel Plan MAY also cover physical information of NAPs, which are not listed in the CAPL.

The following alternatives exist for applying Channel Plans:

- a) no Channel Plans are defined;
- b) only Root Channel Plan is defined;
- c) Root Channel Plan including NAP Based Channel Plan is defined.

Device SHALL support Root Channel Plan. Device MAY support NAP Based Channel Plan as an optimization for NAP discovery and selection.

The device is allowed to select the highest priority NAP of the found NAPs, as dictated by CAPL, after Root Channel Plan based search has been exhausted. The device SHOULD resort to RAPL (i.e. to roam) only in case such NAPs that fit the rules set by CAPL are not found from the bands supported by the device.

An implementation recommendation for Channel Plan and its relationship with CAPL can be found in Annex C4 of [7].

Channel Plan entries MAY be associated with NAPs to specify a NAP Based Channel Plan for a specific NAP. NAP Based Channel Plan may contain references to one or more Channel Plan entries. When a device is configured with a NAP Based Channel Plan and it is carrying out a NAP discovery based on this NAP Based Channel Plan, it is allowed to select this NAP or higher priority NAP from the CAPL.

If the device does not find the NAP using NAP Based Channel Plan and Root Channel Plan, the device MAY ignore the priority of this NAP during further NAP selection process which is done based on NAP Based Channel Plan and Root Channel Plan. When NAP Based Channel Plan is used, it is recommended not to have higher priority NAPs without NAP Based Channel Plan. During the NAP discovery based on NAP Based Channel Plans, the device MAY ignore the priorities of higher priority NAPs which do not have NAP Based Channel Plans.

ANNEX C4 of [7] provides a recommended model for operators to adapt a Channel Plan which is suitable to their network deployment model and device NAP discovery needs.

## Security Parameters

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

## Network deployment mode.

Deployment mode of each NAP, i.e., NAP+NSP mode or NAP sharing mode.

### 4.1.4 SDL

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

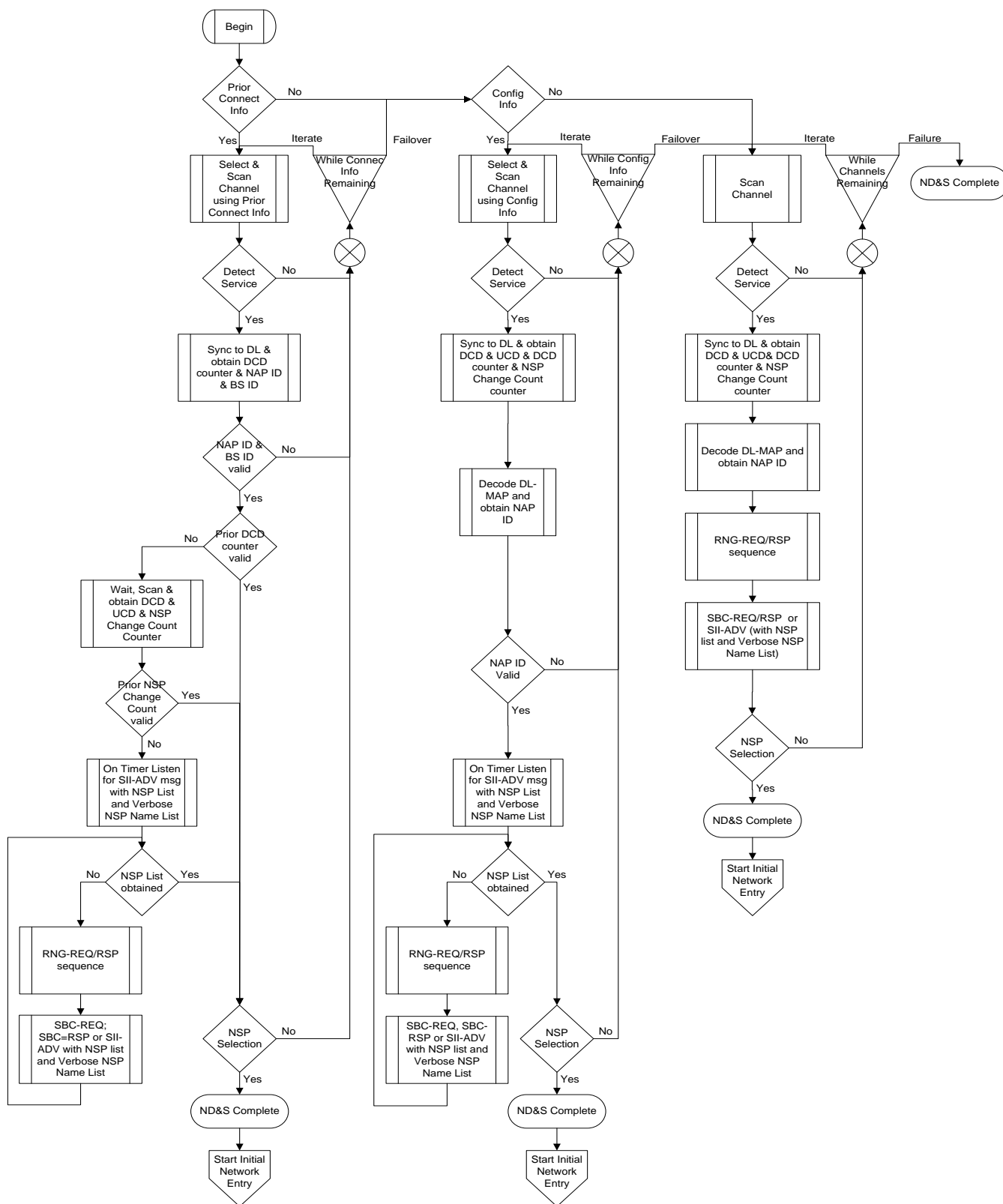


Figure 4-2 – Network Discovery and Selection SDL



#### 4.1.4.1 Process Flow Descriptions

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

#### Process for detection and selection based on stored configuration information of prior base stations

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

- if the MS has stored configuration information of prior base stations' PHY characteristics, suitable and useful for reducing the channel scanning and synchronization options, then the MS uses this information to selectively search for those base stations in 'Select & Scan Channel using Prior Connect Info'.
- else if the MS does not have prior base stations' PHY characteristics, the MS defaults to selection and detection based on more general, account subscription defined configuration information through 'Config Info'.

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

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

- if the MS detects a base station operating with the expected PHY characteristics on the tested channel, the MS proceeds to 'Sync to DL & obtain DCD counter & NAP ID & BS ID'.
- else if the MS fails to detect a BS on the channel, and while untested channels based on the stored configuration remain, the MS repeats the 'Select & Scan Channel using Prior Connect Info' process, iterating to the next channel and BS for assessment; if no untested channels remain, the MS proceeds with detection and selection based on 'Config Info'.

Sync to DL & obtain DCD counter & NAP ID & BS ID': The MS synchronizes to the DL transmissions and obtains the DCD counter from the DL-MAP.

NAP ID & BS ID valid: The MS tests detected NAP ID & BS ID.

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

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

- if the MS determines that the detected DCD counter value matches the stored, expected DCD counter value, then the MS continues to 'NSP Selection'.
- else if the MS determines that the detected DCD counter is different than the stored, expected DCD counter value, the MS SHALL 'Wait, Scan & obtain DCD & UCD & NSP Change Count Counter'.

Wait, Scan & obtain DCD & UCD & NSP Change Count Counter: For MS that detect a DCD counter different than the stored, expected DCD counter value, the MS wait and listen for the transmission of the updated DCD & UCD including NSP Change Count Counter, if present, and continues with 'Prior NSP Change Count valid'.

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

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

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

NSP List obtained: The MS tests for receipt of the list of NSP Ids.

- if the MS obtained the list of NSP IDs, proceed to ‘NSP Selection’.
- else the MS uses the SBC query process to obtain the NSP List, proceed with ‘RNG-REQ/RSP sequence’.

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

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

NSP Selection: The MS conducts automatic NSP selection (see section 4.1.2.3) or manual NSP selection (see section 4.1.2.3).

- if the NAP ID and NSP ID detected will connect the MS to its home CSN for authentication during network entry, and MS decides to do NSP and NAP selection at this point of scanning, the process proceeds to ‘ND&S Complete’.
- else while untested channels based on the stored configuration remain, the MS repeats the ‘Select & Scan Channel using Prior Connect Info’ process, iterating to the next channel and BS for assessment; if no untested channels remain, the MS proceeds with detection and selection based on ‘Config Info’.

ND&S Complete: The MS has successfully completed the network detection and selection process and ‘Start Initial Network Entry’.

Start Initial Network Entry: The MS proceeds with network entry (see section 4.5).

### **Process for detection and selection based on general, account subscription defined stored configuration information**

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

- if the MS has stored configuration information of base stations’ PHY characteristics programmed values obtained as part of the account subscription, suitable and useful for reducing the channel scanning and synchronization options, then the MS uses this information to selectively search for those base stations in ‘Select & Scan Channel using Connect Info’.
- else if the MS does not have prior base stations’ PHY characteristics by subscription programmed values, the MS defaults to selection and detection based on the physical scan capabilities of the MS device through ‘Scan Channel’.

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

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

- if the MS detects a base station operating with the expected PHY characteristics on the tested channel, the MS proceeds to ‘Sync to DL & obtain DCD & UCD & DCD counter & NSP Change Count counter’.
- else if the MS fails to detect a BS on the channel, and while untested channels based on the stored configuration remain, the MS repeats the ‘Select & Scan Channel using Connect Info’ process, iterating to the next channel and BS for assessment; if no untested channels remain, the MS proceeds with detection and selection based on ‘Scan Channel’.

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

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

2 NAP ID valid: The MS tests the detected NAP ID.

3       • if the MS determines that the detected NAP ID matches the stored, expected values, the MS continues

4       ‘On Timer Listen for SII-ADV msg with NSP List and Verbose NSP Name List’.

5       • else if the MS determines that the detected NAP ID does not match the stored, expected value, and

6       while untested channels based on the stored configuration remain, the MS repeats the ‘Select & Scan

7       Channel using Connect Info’ process, iterating to the next channel and BS for assessment; if no

8       untested channels remain, the MS proceeds with detection and selection based on ‘Scan Channel’.

9 On Timer Listen for SII-ADV msg with NSP List and Verbose NSP Name List: During a vendor specific interval

10 timer, the MS listens for the BS transmittal of the SII-ADV message with the NSP List of one or more NSP IDs and

11 Verbose NSP Names.

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

13       • if the MS obtained the list of NSP IDs, proceed to ‘NSP Selection’.

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

15       sequence’.

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

17 SBC-REQ; SBC-RSP or SII-ADV with NSP list and Verbose NSP Name List: The MS conducts SBC-REQ

18 message including SIQ TLV with bit 0 set to a value of ‘1’ during network entry to solicit BS transmittal of NSP

19 List TLV, either through an SII-ADV broadcast or SBC-RSP unicast transmission, and may include SIQ TLV with

20 bit 1 set to a value of ‘1’ during network entry to solicit BS transmittal of Verbose NSP Name List TLV, to be

21 transmitted along with NSP List TLV; the process returns to ‘NSP List obtained’.

22 NSP Selection: The MS conducts automatic NSP selection (see section 4.1.2.3) or manual NSP selection (see

23 section 4.1.2.3).

24       • if the NAP ID and NSP ID detected will connect the MS to its home CSN for authentication during

25       network entry, and MS decides to do NSP and NAP selection at this point of scanning, the process

26       proceeds to ‘ND&S Complete’.

27       • else while untested channels based on the stored configuration remain, the MS repeats the ‘Select &

28       Scan Channel using Connect Info’ process, iterating to the next channel and BS for assessment; if no

29       untested channels remain, the MS proceeds with detection and selection based on ‘Scan Channel’.

30 ND&S Complete: The MS has successfully completed the network detection and selection process and ‘Start Initial

31 Network Entry’.

32 Start Initial Network Entry: The MS proceeds with network entry (see section 4.5).

33 **Process for detection and selection based on physical scan capabilities of the MS device; not**

34 **dependent on stored configuration information**

35 Scan Channel: The MS scans all available channels, limited only by the physical scan capabilities of the MS device;

36 not dependent on stored configuration information.

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

38       • if the MS detects a base station operating on the tested channel, the MS proceeds to ‘Sync to DL &

39       obtain DCD & UCD & DCD counter & NSP Change Count counter’.

40       • else if the MS fails to detect a BS on the channel, and while untested channels based on the physical

41       scan capabilities of the MS device remain, the MS repeats the ‘Scan Channel’ process, iterating to the

42       next channel for assessment; if no untested channels remain, the MS proceeds with detection and

43       selection based on ‘ND&S Complete’ and a result of failure.

44 Sync to DL & obtain DCD & UCD & DCD counter & NSP Change Count counter: The MS synchronizes to the DL

45 transmissions listens for the transmission of the updated DCD & UCD.

1 Decode DL-MAP and obtain NAP ID: The MS listens for and decodes DL-MAP, obtaining the NAP ID.  
2 RNG-REQ/RSP sequence: The MS conducts RNG-REQ/RSP as defined in IEEE Std 802.16.  
3 SBC-REQ, SBC-RSP or SII-ADV with NSP list and Verbose NSP Name List: The MS conducts SBC-REQ; then  
4 MS transmits SBC-REQ including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS  
5 transmittal of NSP List TLV, either through an SII-ADV broadcast or SBC-RSP unicast transmission, and may  
6 include SIQ TLV with bit 1 set to a value of '1' during network entry to solicit BS transmittal of Verbose NSP  
7 Name List TLV, to be transmitted along with NSP List TLV proceed with 'NSP Selection'.  
8 NSP Selection: The MS conducts automatic NSP selection (see section 4.1.2.3) or manual NSP selection (see  
9 section 4.1.2.3).  
10       • if the NAP ID and NSP ID detected will connect the MS to its home CSN for authentication during  
11       network entry, and MS decides to do NSP and NAP selection at this point of scanning, the process  
12       proceeds to 'ND&S Complete'.  
13       • else while untested channels remain, the MS repeats the 'Scan Channel' process, iterating to the next  
14       channel and BS for assessment; if no untested channels remain, the MS proceeds with 'ND&S  
15       Complete' and a result of failure.  
16 ND&S Complete: The MS has successfully completed the network detection and selection process and 'Start Initial  
17 Network Entry'.  
18 Start Initial Network Entry: The MS proceeds with network entry (see section 4.5).

## 19 4.2 IP Addressing

### 20 4.2.1 IPv4 Addressing

21 Functional entities and architecture for IPv4 addressing are described in Stage 2 section 7.2.1. Details on how IPv4  
22 addressing is performed via DHCP, PMIP4, PMIP6, and CMIP4 are described in Stage 3 section 4.8. Details on how  
23 IPv4 addressing is performed for Simple IP is described in Stage 3 Section 4.13.

### 24 4.2.2 IPv6 Addressing

25 IPv6 addressing details are described in Stage 3 section 4.11. Addressing principles and restrictions for PMIP6 are  
26 described in Stage 2 section 7.2.2.5. Details on how addressing is performed via stateless address autoconfiguration  
27 and DHCPv4 or DHCPv6 are specified in Stage 3 section 4.8.5.

## 28 4.3 WiMAX Key Hierarchy and Distribution

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

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

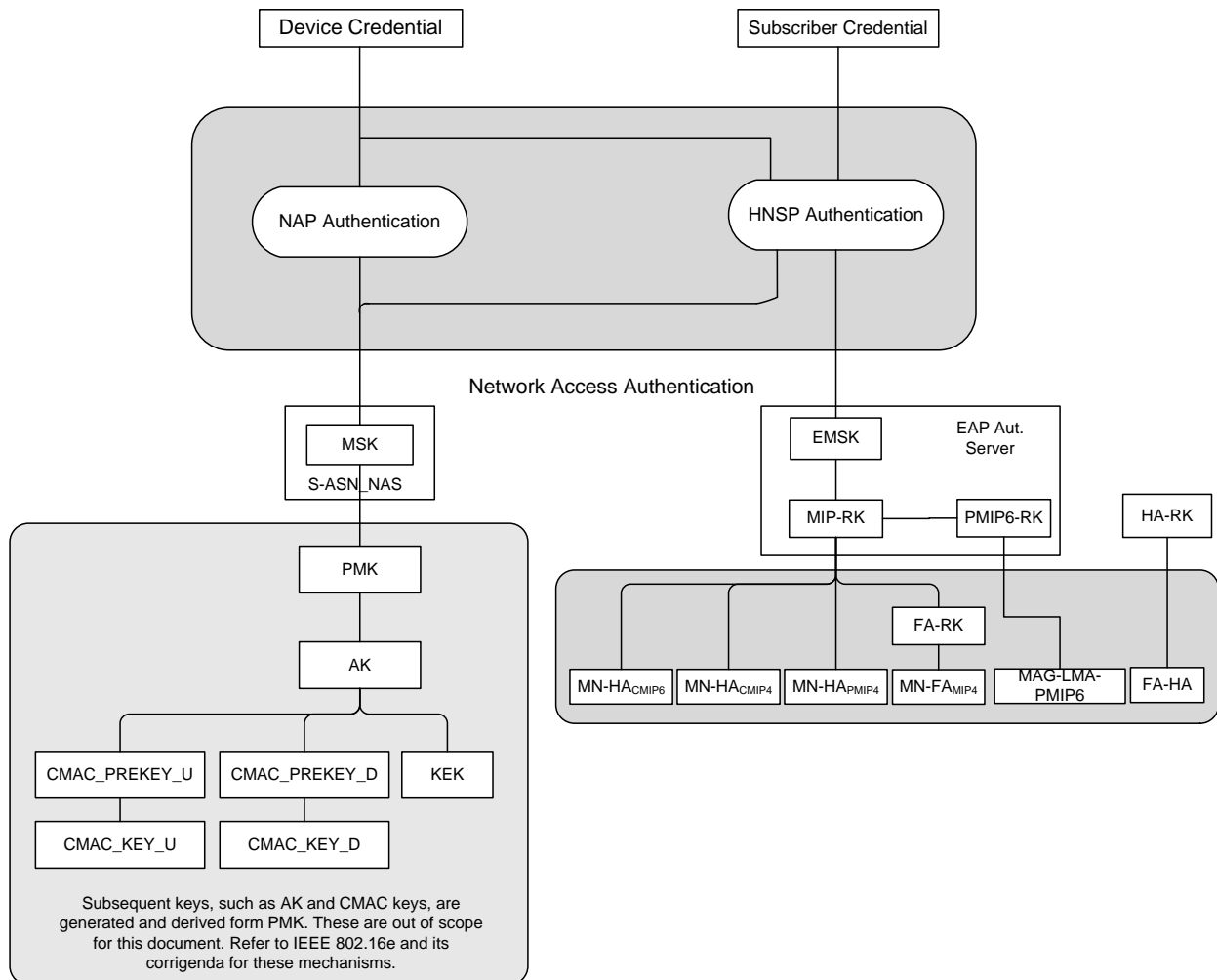
33 A device credential MAY also be used as a subscriber credential. That is possible when the subscriber is identified  
34 by the MAC address of the device. In that special case, a single credential provisioned in the device can be used for  
35 authenticating both the device and the subscriber at the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

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

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

42 The MS and the network perform authentication using EAP ([56]). The EAP method selected SHALL be capable of  
43 producing MSK and EMSK.

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



**Figure 4-3 – WiMAX Key Hierarchy**

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

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

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

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

For the PMIP6 in-band security, a PMIP6-RK SHALL be generated at the AAA from MIP-RK. The PMIP6-RK keys generated at the HAAA are transported to the LMA, and the Authenticator by the use of the AAA protocol when this is required. The PMIP6 security keys used for in-band security protection of PBU/PBA are then generated at both the Authenticator and LMA from the PMIP6-RK.

#### 4.3.1 Mobile IP Root Key (MIP- RK)

The Mobile IP Root Key (MIP-RK) is generated at the EAP-Authentication Server which is collocated with the 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:

$$\text{MIP-RK-1} = \text{HMAC-SHA256}(\text{EMSK}, \text{usage-data} \parallel 0x01)$$

$$\text{MIP-RK-2} = \text{HMAC-SHA256}(\text{EMSK}, \text{MIP-RK-1} \parallel \text{usage data} \parallel 0x02)$$

$$\text{MIP-RK} = \text{MIP-RK-1} \parallel \text{MIP-RK-2}$$

where:

$$\text{usage-data} = \text{key label} + "\backslash 0" + \text{length}$$

$$\text{key label} = \text{miprk@wimaxforum.org} \text{ in ASCII}$$

$$\text{length} = 0x0200 \text{ the length in bits of the MIP-RK expressed as a 2 byte unsigned integer in network order}$$

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

The MIP-RK is stored in the HAAA and CMIP capable MS.

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

The 64 octet PMIP6-RK SHALL be generated from the MIP-RK using the following formula:

$$\text{PMIP6-RK-1} = \text{HMAC-SHA256}(\text{MIP-RK}, \text{usage-data} \parallel 0x01)$$

$$\text{PMIP6-RK-2} = \text{HMAC-SHA256}(\text{MIP-RK}, \text{PMIP6-RK-1} \parallel \text{usage data} \parallel 0x02)$$

$$\text{PMIP6-RK} = \text{PMIP6-RK-1} \parallel \text{PMIP6-RK-2}$$

where:

$$\text{usage-data} = \text{key label} + "\backslash 0" + \text{length}$$

$$\text{key label} = \text{pmip6rk@wimaxforum.org} \text{ in ASCII}$$

$$\text{length} = 0x0200 \text{ the length in bits of the PMIP6-RK expressed as a 2 byte unsigned integer in network order}$$

The lifetime of PMIP6-RK MUST be set to the lifetime of MIP-RK.

The PMIP6-RK is stored in the HAAA and SHALL be sent to both anchor authenticator and the corresponding LMA.

The PMIP6-RK is used to generate the MAG-LMA-PMIP6 key (see section 4.3.2).

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

$$\text{MIP-SPI} = \text{the 4 most significant bytes of HMAC-SHA256}(\text{MIP-RK} \text{ "SPI CMIP PMIP"})$$

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.g. all collisions with any active

SPI values related to the 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

SPI-PMIP6 = MIP-SPI + 3

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**

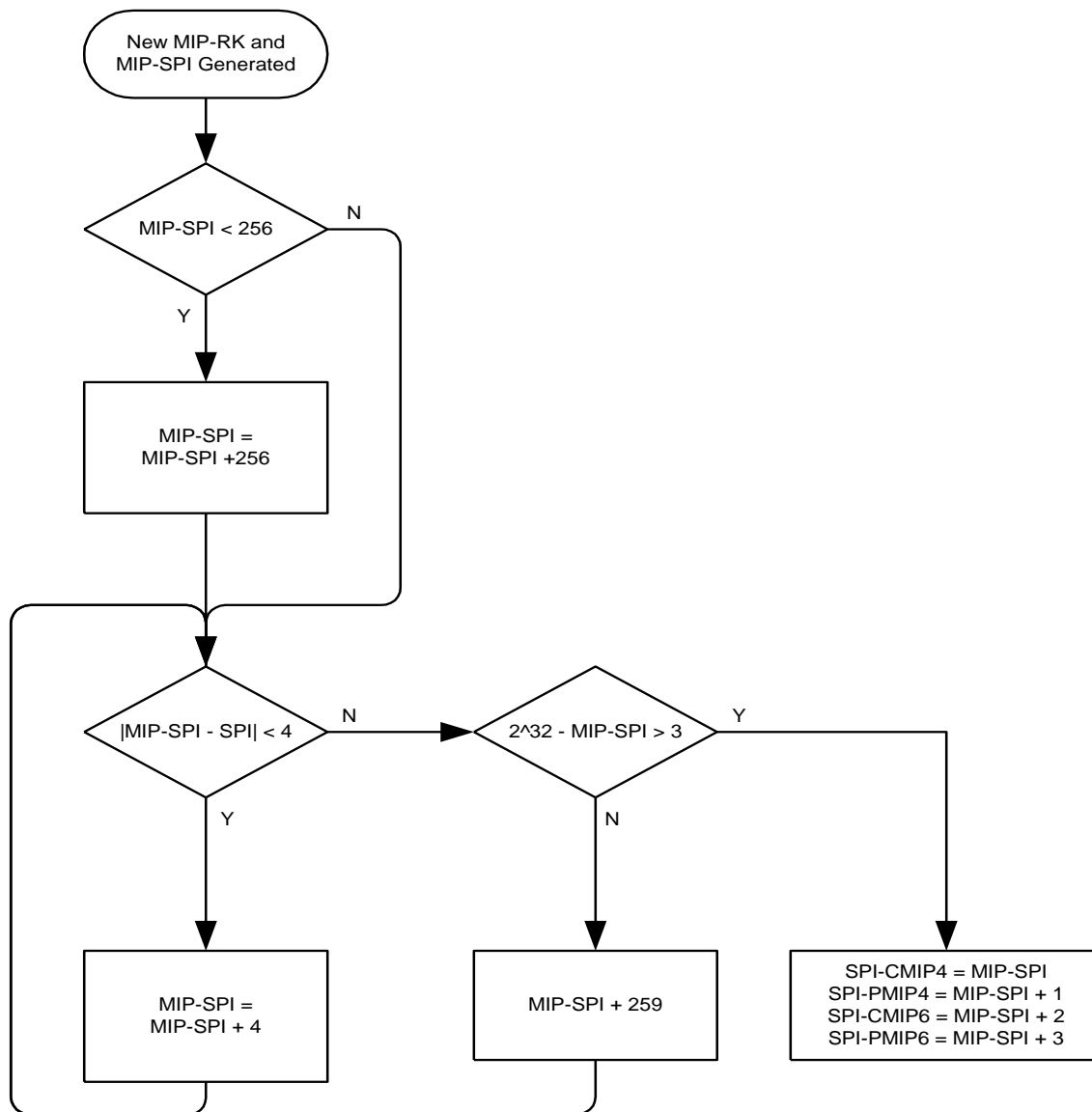
The following procedure prevents collision between SPI values used for different Mobility keys, for example, mobility keys used by other access technologies, during the same Mobile IP session. The procedure SHALL be executed as follows:

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 ( $2^{32} - 1$ ), 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.



**Figure 4-4 – SPI Collision Avoidance Mechanism**

#### 4.3.1.2 Key Distribution

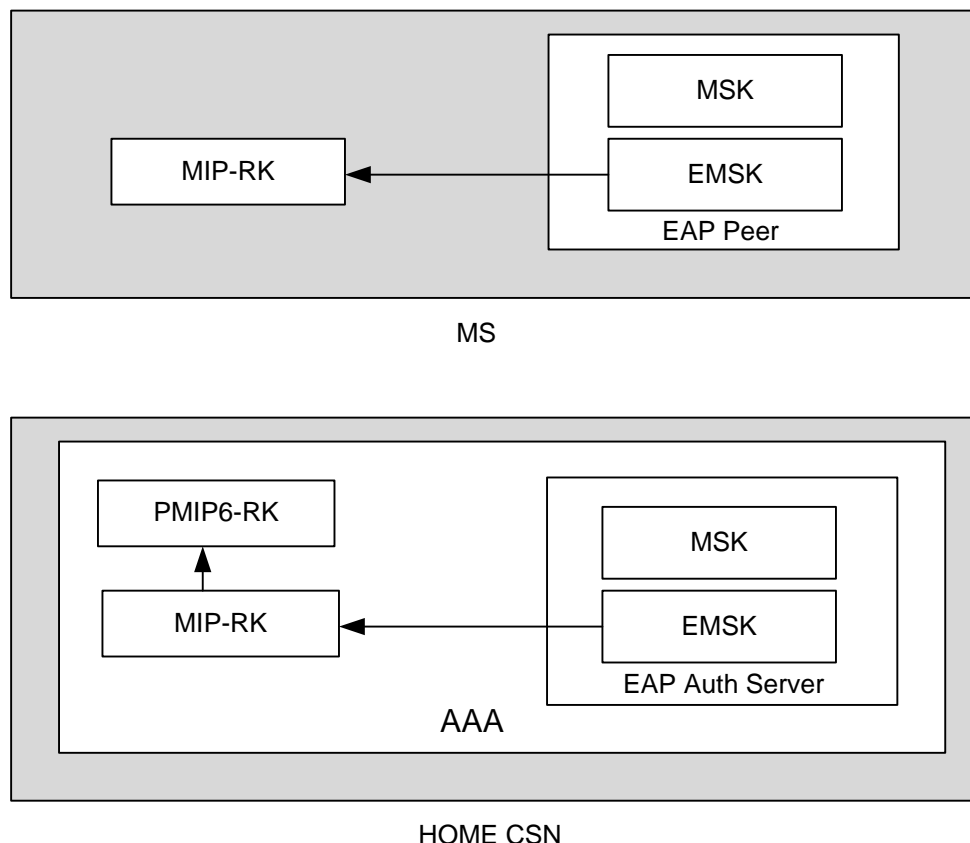
As specified above, the MIP-RK key is derived at the MS and the HAAA at the CSN and does not get distributed outside those entities.

The PMIP6-RK key is derived at the HAAA at the CSN and distributed to the Anchor Authenticator in the NAS and to the LMA along with its associated SPI-PMIP6. The SPI-PMIP6 is used by the MAG, LMA, and HAAA to identify the PMIP6-RK and the derived MAG-LMA-PMIP6 key to compute the Authentication Option in the PBU/PBA.

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, FA-RK-SPI is set to the same value of SPI-CMIP4 and is distributed to the NAS during Access Authentication, in AAA 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 authenticator 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.



**Figure 4-5 – Key Distribution**

#### 4.3.1.3 Key Deprecation

Mobile IP keys (MIP-RK, PMIP6-RK, MN-HA, FA-RK, MN-FA, HA-RK, FA-HA, MAG-LMA-PMIP6) SHALL NOT be used after their individual lifetime expires.

When the newer version of a key is generated/distributed, a network element MAY conclude that the previous version of the key is no longer needed through a key rollover confirmation process. Under such circumstances, the previous version of the key is deemed deprecated and SHALL NOT be used anymore even though its lifetime may not have expired yet. Specifically, when the MS re-authenticates and a new MIP-RK is generated, old MIP-RK and its derivatives (PMIP6-RK, MN-HA, FA-RK, MN-FA, MAG-LMA-PMIP6) 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. For the Proxy Mobile IPv6 PBU and PBA signed by the new MAG-LMA-PMIP6 key identified by the new SPI-PMIP6 SHALL be used by the MAG to deprecate the old MAG-LMA-PMIP6 key, and trigger the authenticator, LMA and HAAA to deprecate the old PMIP6-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; two-way use of FA-HA key SHALL prompt FA and HA to deprecate the old FA-HA key.

1 Additionally, MIP-RK, PMIP6-RK, MN-HA, FA-RK, MAG-LMA-PMIP6, and MN-FA keys SHALL be  
2 deprecated as soon as the MS session terminates (i.e., ASN generates the final RADIUS Accounting Stop, or  
3 Diameter WSTR and WACR commands).

4 HA-RK and its context SHALL be deleted by the HA and AAA servers only after its lifetime expires. HA-RK and  
5 its context MAY be deleted by the Authenticator if a new HA-RK context with longer lifetime is received for the  
6 MIP sessions associated with the same HA. Also, if the Authenticator receives the new HA-RK context which has a  
7 shorter lifetime than the one already available, the Authenticator MAY delete the newly received HA-RK context. If  
8 the FA receives the new FA-HA context which has the lifetime shorter than the one already available, the FA MAY  
9 delete the newly received FA-HA context.

#### 10 **4.3.2 AK Key**

11 The AK key is derived from the PMK key at the NAS (MSK was transported to the NAS via the AAA  
12 infrastructure). AK is derived using the method specified in [11] where PMK and EIK are generated.

##### 13 **4.3.2.1 Key Generation**

14 MSK is 512 bits long. PMK and is 160 bits long.

15 PMK is derived from the MSK. The PMK and EIK derivation from the MSK is as follows:

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

17 AK will be derived by the MS and the NAS from the PMK.

18 `AK = Dot16KDF(PMK, MS MAC Address | BSID | "AK", 160);`

##### 19 **4.3.2.2 Key Lifetime**

20 AK lifetime equals the PMK remaining lifetime.

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

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

#### 25 **4.3.3 AK SN, PMK SN Usage and AK Context**

##### 26 **4.3.3.1 Clarification of AK SN and PMK SN**

27 PMK SN is a 4 bit values.

28 The least significant 2 bits of PMK SN represent the sequence counter, and the most significant 2 bits always set to  
29 zero. AK SN is equal to the PMK SN, only the least significant 2 bits are used, the most significant 2 bits SHALL  
30 always set to zero.

##### 31 **4.3.3.2 PMK SN Usage in Initial Authentication**

32 The least significant 2 bits of PMK SN SHALL be initialized to zero.

##### 33 **4.3.3.3 PMK SN Usage in Re-authentication**

34 When re-authentication is successfully completed, the least significant 2 bits of PMK SN SHALL be incremented by  
35 1 modulo 4.

##### 36 **4.3.3.4 AK SN Derivation from PMK SN**

37 AK SN is a 4 bit value. The least significant 2 bits SHALL be used as the sequence counter.

38 AK SN SHALL equal PMK SN.

39 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<sub>M</sub> or  $X$ , the count value maintained by the BS is denoted as CMAC\_KEY\_COUNT<sub>B</sub> or  $Y$ , and the value maintained by the Anchor Authenticator is denoted as CMAC\_KEY\_COUNT<sub>N</sub> or  $Z$ .

##### 4.3.4.1 Maintenance of CMAC\_KEY\_COUNT<sub>M</sub> 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<sub>M</sub> ( $X$ ) to zero. In particular, this reset SHALL occur upon reception of the SA-TEK Challenge message. The MS SHOULD initiate re-authentication when the CMAC\_KEY\_COUNT<sub>M</sub> reaches a value of 32768. Note, that MS SHALL manage a separate CMAC\_KEY\_COUNT<sub>M</sub> for every active PMK context. Specifically, during reauthentication, after EAP completion, but before the new PMK activation, the old CMAC\_KEY\_COUNT<sub>M</sub> (as per old PMK) is used for CMAC generation of MAC control messages, while the new CMAC\_KEY\_COUNT<sub>M</sub> (which is initialized from zero) is used for CMAC generation for PKMv2 3-way handshake messages. The old CMAC\_KEY\_COUNT<sub>M</sub> 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<sub>M</sub> counter ( $X++$ ). The MS SHALL send the value of the CMAC\_KEY\_COUNT<sub>M</sub> ( $X$ ) 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<sub>M</sub> cannot be changed. In other words, while in the CMAC\_Key\_Lock state, the MS SHALL use the same value of CMAC\_KEY\_COUNT<sub>M</sub> 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<sub>N</sub> ( $Z$ ) 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<sub>B</sub> ( $Y$ ). 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

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

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

If the BS does not possess the value of  $\text{CMAC\_KEY\_COUNT}_B$  ( $Y$ ) as will always be the case in the Uncontrolled HO, it SHALL request and receive it from the Anchor Authenticator. As an example, the BS MAY use the *Context\_Req* / *Context\_Rpt* transaction for this purpose.

If the BS obtains the AK Context including the  $\text{CMAC\_KEY\_COUNT}_N$  ( $Z$ ) from the Anchor Authenticator, the BS SHALL set  $\text{CMAC\_KEY\_COUNT}_B = \text{CMAC\_KEY\_COUNT}_N$  ( $Y = Z$ ).

Upon receiving the RNG-REQ message from the MS containing the  $\text{CMAC\_KEY\_COUNT}$  TLV, the BS SHALL compare the received count value  $\text{CMAC\_KEY\_COUNT}_M$  with the  $\text{CMAC\_KEY\_COUNT}_B$  ( $X <> Y$ ).

If  $\text{CMAC\_KEY\_COUNT}_M < \text{CMAC\_KEY\_COUNT}_B$ , and the RNG-REQ message is received as a part of reentry or HO, the BS SHALL send the RNG-RSP message rejecting an access and indicating that MS SHALL conduct full re-authentication.

If  $\text{CMAC\_KEY\_COUNT}_M \geq \text{CMAC\_KEY\_COUNT}_B$ , the BS SHALL do the following:

The BS SHALL use the  $\text{CMAC\_KEY\_COUNT}_M$  to compute a temporary value of  $\text{CMAC\_KEY\_U}_T$ , and use the  $\text{CMAC\_KEY\_U}_T$  to validate the CMAC digest present in the RNG-REQ message.

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

- If the CMAC digest is valid, and  $\text{CMAC\_KEY\_COUNT}_M = \text{CMAC\_KEY\_COUNT}_B$ , the BS SHALL send the RNG-RSP message to the MS allowing legitimate access. Once an access is completed, the BS SHALL inform the Anchor Authenticator of the successful access by using, the R6 *CMAC\_Key\_Count\_Update* message.
- If CMAC digest is valid, and  $\text{CMAC\_KEY\_COUNT}_M > \text{CMAC\_KEY\_COUNT}_B$ , the BS SHALL send the RNG-RSP message to the MS allowing legitimate access. Once an access is completed, the BS SHALL inform the Anchor Authenticator of the successful access by using the R6 *CMAC\_Key\_Count\_Update* message and include the  $\text{CMAC\_KEY\_COUNT}_M$  in the message.

#### 4.3.4.2.2 Processing of $\text{CMAC\_KEY\_COUNT}$ by the Anchor Authenticator

The Anchor Authenticator SHALL maintain the  $\text{CMAC\_KEY\_COUNT}_N$  for every MS as part of its security context, called the AK Context, and associated with the PMK. When the Anchor Authenticator for the MS is relocated, and the associated AK context for the MS is deleted in the old Anchor Authenticator, the value of  $\text{CMAC\_KEY\_COUNT}_N$  is also deleted.

Upon successful completion of the PKMv2 Authentication or Re-authentication, and creation of a new PMK, the Anchor Authenticator SHALL set the  $\text{CMAC\_KEY\_COUNT}_N$  for the MS to 1. In particular, setting the count to 1 SHALL occur when the Authenticator receives indication about the successful completion of EAP-based authentication. The Anchor Authenticator SHALL never set the value to zero and only reset the value to 1 after a new PMK has been established.

Upon receiving the *Context\_Req* message containing a request for the AK from the BS, the Anchor Authenticator SHALL return the current value of the  $\text{CMAC\_KEY\_COUNT}_N$  in the *Context\_Rpt* message.

Upon receiving the indication of the successful access from the BS in the R6 *CMAC\_Key\_Count\_Update* message containing the  $CMAC\_KEY\_COUNT_M$ , the Anchor Authenticator SHALL compare it to the locally maintained value of  $CMAC\_KEY\_COUNT_N$  and select the largest of the two as the valid value of the count, such that

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

in other words,

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

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

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

This section exemplifies several error case scenarios.

##### 4.3.4.3.1 Handover Cancellation

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

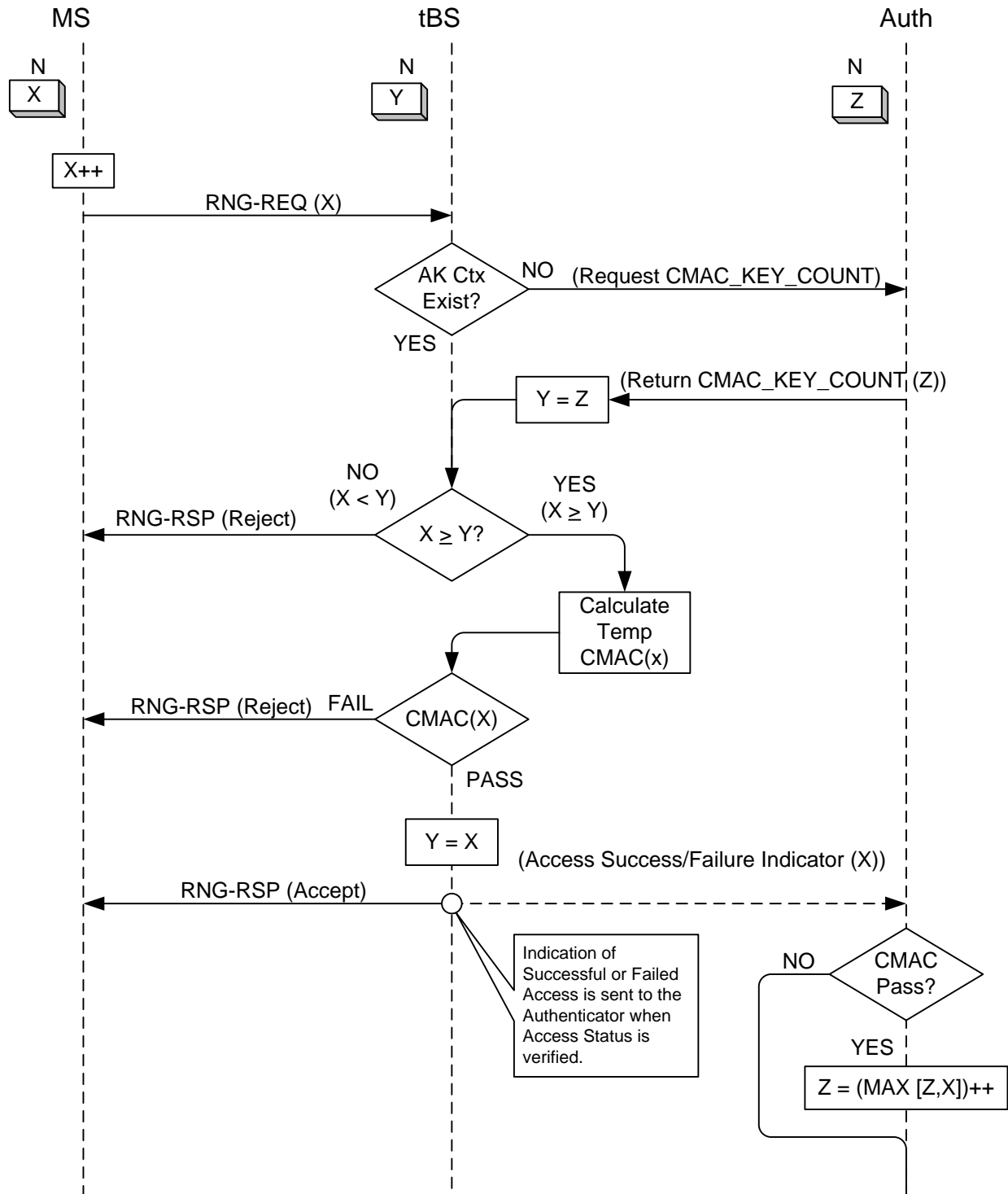
##### 4.3.4.3.2 Handover Failure

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

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

##### 4.3.4.4 Process Flowchart

This section shows a simplified process flowchart for reentry, handover, or Secure Location Update.



**Figure 4-6 – Replay Protection for Reentry, Handover, and Secure Location Update**

### 4.3.5 MIP Keys

MIP Keys used for Mobility Authentication are generated from the MIP-RK. These include keys for CMIP4, PMIP4, CMIP6 and PMIP6. The MIP keys are generated at the HAAA and at the MS. The keys generated at the

HAAA are transported to the HA, LMA, the Authenticator, and the PMIP client by the use of the AAA protocol when this is required. Keys generated at the MS are not distributed.

#### 4.3.5.1 Key Generation

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

When EAP-Re-authentication occurs, a new MIP-RK is generated, including the derived MN-HA, PMIP6-RK and FA-RK mobility keys.

In the computation of the formulas specified in this section the following encoding SHALL be used:

- All quoted strings (e.g., “CMIP4 MN HA”) are binary representation of the UTF8 encoding of the non-null terminating strings (case sensitive).
- All IPv4 addresses are the 32-bit binary representation of the IPv4 address in network byte order.
- All IPv6 addresses are the 128-bit binary representation of the IPv6 address in network byte order.
- All SPIs are 32-bit unsigned integers in network byte order.
- All NAIs (e.g., MN-NAI) are binary representation of the UTF8 encoding of the non-null terminating NAI string (case sensitive) provided in the MIP Registration / Binding.

The derivation of mobility keys are given below:

$$\text{MN-HA-CMIP4} = \text{H}(\text{MIP-RK}, \text{“CMIP4 MN HA”} \mid \text{HA-IPv4} \mid \text{MN-NAI})$$
$$\text{MN-HA-PMIP4} = \text{H}(\text{MIP-RK}, \text{“PMIP4 MN HA”} \mid \text{HA-IPv4} \mid \text{MN-NAI})$$
$$\text{MN-HA-CMIP6} = \text{H}(\text{MIP-RK}, \text{“CMIP6 MN HA”} \mid \text{HA-IPv6} \mid \text{MN-NAI})$$
$$\text{MAG-LMA-PMIP6} = \text{H}(\text{PMIP6-RK}, \text{“PMIP6 MAG LMA”} \mid \text{MAG-IPv6} \mid \text{LMA-IPv6} \mid \text{MN-NAI})$$

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

As MN roams from one FA to another, its security association with HA stays unchanged, and therefore is bound 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.

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

The lifetime of all MAG-LMA-PMIP6 keys SHALL be set to the lifetime of the PMIP6-RK.

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

The PMIP6-RK-SPI value associated with PMIP6-RK is the same as SPI-PMIP6 generated at the time of generating PMIP6-RK, as specified in section 4.3.1.1.

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

$$\text{FA-RK} = \text{H}(\text{MIP-RK}, \text{“FA-RK”})$$
$$\text{MN-FA} = \text{H}(\text{FA-RK}, \text{“MN FA”} \mid \text{FA-IP} \mid \text{MN-NAI})$$

The FA-RK is generated by the HAAA and distributed to the authenticator as specified in section 4.3.5.3. It is used by the authenticator to derive MN-FA keys as requested by the FA. If a handover to a new FA takes place without re-authentication, the anchor authenticator holding the FA-RK is responsible to generate and provision MN-FA to the new FA on request. The MN-FA key is derived based on the FA-IP address to separate keys between different

FAs for the same authentication session. The lifetime of FA-RK and MN-FA SHALL be set to the lifetime of the MIP-RK.

The FA-RK-SPI value is set to the same value of SPI-CMIP4 as described in section 4.3.1.2. The SPI associated with the MN-FA (MN-FA-SPI) is set to the same value of FA-RK-SPI distributed during Access Authentication as described in section 4.3.1.2.

The HA-RK and its context is created by the AAA server assigning the HA to an authenticating subscriber. The context includes its SPI and lifetime. A different 160-bit random HA-RK and its context including associated SPI and lifetime is created for every HA on a per-authenticator basis. For example, if the same HA is allocated for two different MIP session authenticated through two different authenticators, then the AAA server creates two different HA-RK keys and their associated context.

The HA-RK and its associated context is distributed to the authenticator and to the HA as specified in section 4.3.5.2 to derive FA-HA keys.

If the authenticator receives the new HA-RK for a given HA session with the lifetime that expires sooner than the lifetime of another HA-RK already available at the authenticator for the same HA, the authenticator MAY discard the new HA-RK and its context. If the authenticator receives the new HA-RK for a given HA session with the lifetime that is longer than the lifetime of another HA-RK already available at the authenticator for the same HA, the authenticator MAY discard the older HA-RK and its context.

The HA SHALL retain all HA-RK keys and their context until their lifetime expires.

An FA-HA key is generated by the HA, and by the authenticator for a specific pair of HA and this FA.

$$FA-HA = H(HA-RK, "FA-HA" \parallel HA-IPv4 \parallel FA-CoAv4 \parallel SPI)$$

The FA-HA is computed as a hash (HMAC-SHA1) of the following (in hex):

- HA-RK, a random 160-bit number used as the key followed by the concatenation of the following:
  - o the binary representation of the non null terminated string "FA-HA"
  - o HA-IPv4 is a 32-bit binary representation of the IP address in network byte order
  - o FA-CoAv4 is a 32-bit binary representation of the IP address in network byte order
  - o SPI is a 32-bit unsigned integer in network byte order

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

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 specific EAP authentication. Hence, they are not bound to individual user or authentication sessions. HA-RK and FA-HA keys are only generated on demand, but not for each EAP (re-)authentication or MIP registration taking place. Nevertheless, HA-RK key along with the SPI and lifetime values are delivered to the authenticator during network access authentication of a MS (i.e., it is piggybacked). The lifetime and SPI of HA-RK is managed by the AAA server assigning the HA. It is the responsibility of the AAA to generate and deliver a new HA-RK to the authenticator prior to the expiration of the HA-RK. To avoid potential loss of the HA-RK in transmission, and as the result, possible absence of a valid HA-RK at the Authenticator, the AAA SHALL send the HA-RK and its context with every EAP authentication procedure. During any EAP authentication procedure, if AAA finds that the remaining lifetime of HA-RK is less than the new MSK lifetime assigned, RADIUS Access-Accept or Diameter WDEA command message SHALL contain a new HA-RK and its context. AAA servers SHALL make sure that HA-RK lifetime is longer than MSK lifetime. The same SPI value is used symmetrically (i.e., both in MIP RRs and MIP RRs).

H()	HMAC-SHA1 [23]
HA-IPv4	IP address expressed as a 32-bit binary value of the HA in network byte order as seen from the FA and as reported in the Mobile messages.
FA_CoAv4	Address of the FA expressed as a 32-bit binary value in network byte order as seen by the HA.
FA-IP	Address of the FA expressed as a 32-bit binary value in network byte order as seen by the MS.



HA-IPv6	IPv6 address expressed as a 128-bit binary value of the HA in network byte order as seen from the MN and as reported in the Mobile messages.
MAG-IPv6	IPv6 address expressed as a 128-bit binary value of MAG in network byte order as seen by the LMA (the IPv6 source address of the PBU).
LMA-IPv6	IPv6 address expressed as a 128-bit binary value of the LMA in network byte order as seen by the MAG (the IPv6 source address of the PBA).
MN-NAI	User NAI provided in the MIP Registration Request.

The lengths of the resulting keys are 160-bits.

#### 4.3.5.2 Key Generation Example

The following is an example of key generation using the algorithms described in 4.3.5.1.

Given that the EMSK key, NAI, HA MIP4 address and SPIs have the following values:

EMSK = 00112233445566778899AABBCCDDEEFF

00112233445566778899AABBCCDDEEFF

00112233445566778899AABBCCDDEEFF

00112233445566778899AABBCCDDEEFF

NAI = 00112233445566778899AABBCCDDEEFF@example.com

HA-IP-MIP4 = 10.0.0.1

MIP-SPI = 204743442

SPI-PMIP4 = 204743443

The generated keys are listed as follows:

MIP-RK = 0x2C5D24FAB7D88D15754006E00416FABB

58DBA67DB2D3ED9B6A225A011228479E

8990358CEE25031008EFD8A80EBCCB70

99B009E3C550309747A35DB63DFD9EAC

MN-HA-PMIP4 = 0xA6D592C12B090E5923F0A4B2B9503CDA3350A46E

The following is an example of FA-HA key generation using the algorithms described in 4.3.5.1.

“FA-HA” = 0x46412D4841

HA-IPv4 = 131.213.64.3 = 0x83D54003

FA-CoAv4: 47.104.241.97 = 0x2F68F161

SPI: 5000 = 0x00001388

Given HA-RK: 0x000102030405060708090A0B0C0D0E0F10111213

Generated key is as under:

FA-HA = 0x041CFF52F88D4E596D65628392317A12169BC47E

#### 4.3.5.3 Key Distribution

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

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

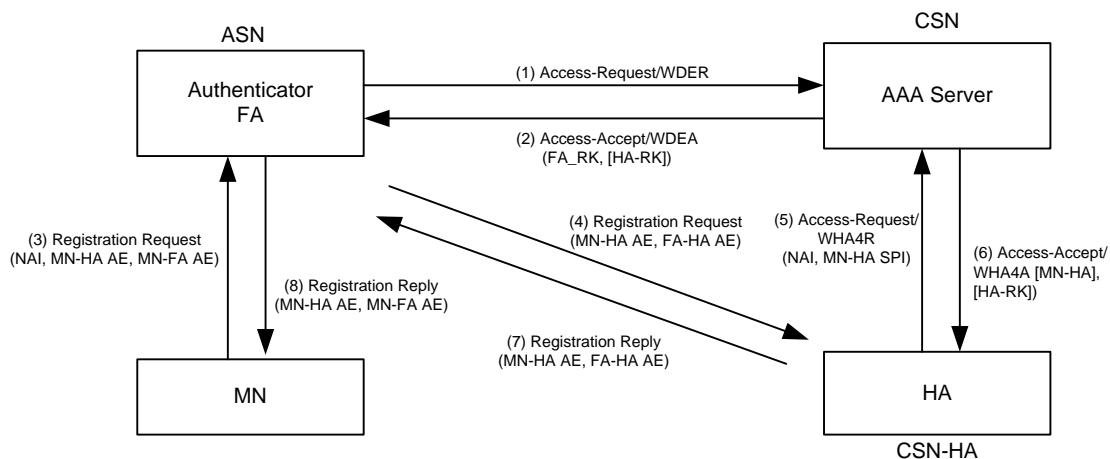
Key	Generated by	Used at
MN-HA-CMIP4	MN and HAAA	HA and MN
MN-HA-PMIP4	HAAA	HA and PMIP4 client
MN-HA-CMIP6	MN and HAAA	MN and HA
FA-RK	MN and HAAA	MN and Authenticator
MN-FA	MN and Authenticator	FA and MN
HA-RK	HAAA or VAAA	HA and Authenticator
FA-HA	HA and Authenticator	HA and FA
PMIP6-RK	HAAA	LMA and Authenticator
MAG-LMA-PMIP6	LMA and Authenticator	MAG and LMA

The keys that are used by the MN are generated by the MN and SHALL NOT be transported outside the MN. The keys generated by the HAAA are transported to the HA or the Authenticator using AAA protocols (RADIUS/Diameter).

#### 4.3.5.3.1 Key Distribution for CMIP4

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

Figure 4-7 illustrates the key distribution for CMIP4.



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

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

For CMIP, the MIP4 Client resides in the MS and the FA resides in the ASN. The location of the HA is shown such that it could be in the home network (in which case the AAA broker does not exist) or in a visited CSN in which case there could be one or more AAA brokers between it and the HAAA server though it is not shown in Figure 4-7.

1 The MIP4 Client in the MS receives the MN-FA and MN-HA-CMIP4 keys along with the SPIs and lifetimes that  
2 were generated by the MS from the MIP-RK key during EAP based Device/User Authentication.

3 The following key distribution scheme applies:

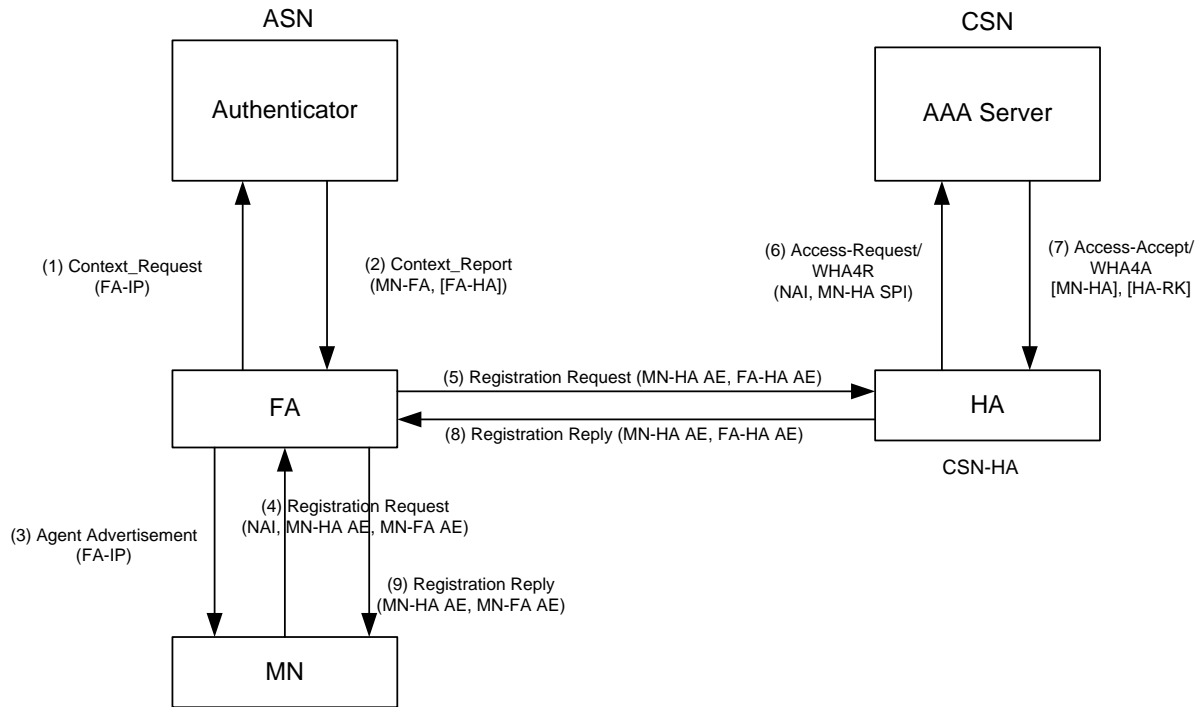
4 The authenticator receives a set of mobility keys and other keys in the RADIUS Access-Accept packet or Diameter  
5 WDEA command as a result of successful authentication. These include FA-RK, and HA-RK (with its SPI and  
6 lifetime). MN-HA-CMIP4 SHALL NOT be sent to the authenticator by the HAAA. In the case of RADIUS, the  
7 keys are encrypted using the method defined in [42] section 3.5. In the case of Diameter, the keys are protected by  
8 the transport security mechanism (IPsec or TLS). The AAA messages MAY be transported through one or more  
9 AAA brokers or proxies. The keys are stored at the authenticator.

10 At the time of CMIP4 procedures, the FA obtains the MN-FA key and, if required, the FA-HA key it needs from the  
11 authenticator. If this is a new FA after re-location without re-authentication, the new FA requests the keys by  
12 sending a Context\_Req message to the anchor authenticator if these keys are required. The FA SHALL set bit#8 in  
13 the Context Purpose Indicator TLV for requesting an MN-FA context, and bit#9 for requesting a FA-HA context.  
14 Upon receiving such Context\_Req message from the FA, the anchor authenticator SHALL reply with a Context\_Rpt  
15 message including a MIP4 Security Info TLV to carry the requested keys. The authenticator derives MN-FA from  
16 FA-RK and, if required, FA-HA from HA-RK according to the procedures given in section 4.3.5.1.

17 After re-authentication occurs, the Authenticator SHALL send the new security context to the Anchor DPF/FA in  
18 the Context\_Rpt message. The new security context may include MN-FA with associated SPI value if MN-FA  
19 authentication is required, and the FA-HA key with associated SPI values if FA-HA authentication is required.

20 Upon receipt of an MIP-RRQ from the MS, if MN-FA is required, the FA SHALL determine whether re-  
21 authentication has occurred since the last MIP-RRQ by comparing the SPI contained in the MN-FA Authentication  
22 extension of the received MIP-RRQ to the locally stored value of MN-FA SPI. If the two SPIs are different, the FA  
23 SHALL assume that re-authentication has occurred, and the new MN-FA key SHALL be retrieved from the  
24 authenticator.

25 In the case of re-authentication due to authenticator relocation, and if MN-FA is required, the FA may send context  
26 request to the old authenticator after receiving the MIP-RRQ with the different SPI value. If the old authenticator  
27 receives such context request, it SHALL respond with error code (Failure Indication TLV) and with the ID of the  
28 new authenticator, so that the FA can retrieve the new MN-FA key from the new authenticator.



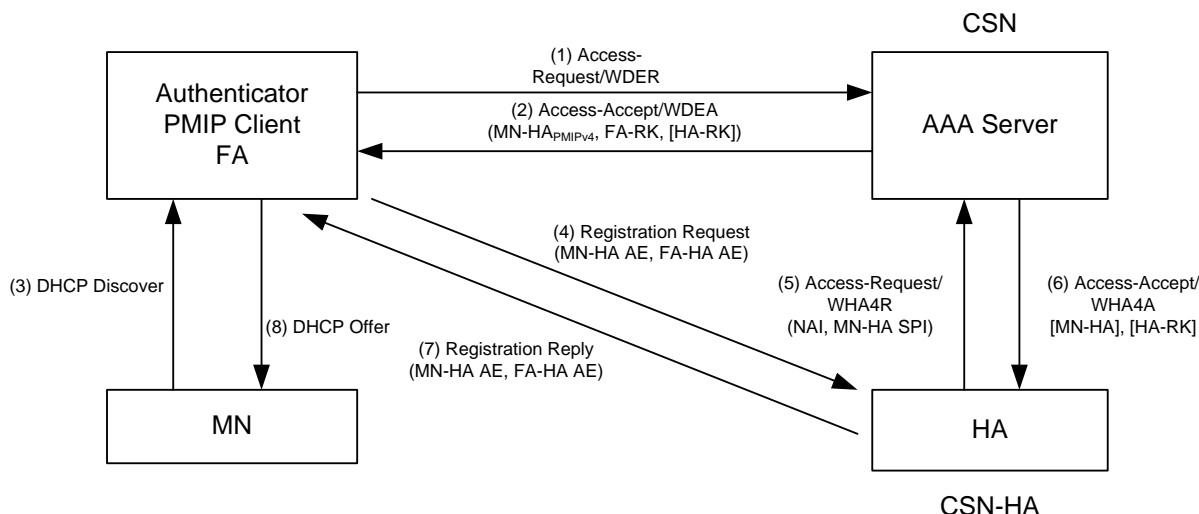
**Figure 4-8 – CMIP4 Key Distribution with FA Relocation**

The HAAA distributes the MN-HA key and the HA-RK key, if requested, to the HA using RADIUS Access-Accept or Diameter WH4A command. For MN-HA, the HAAA sends the MN-HA-CMIP4 key to the HA when the SPI used in the MIP Registration Request is associated with CMIP MN-HA key (equal to SPI-CMIP4). The HA requests and uses these keys for verification of MN-HA AE and FA-HA AE according to the procedures described in section 4.8. Any new FA-HA key is derived in the HA from HA-RK according to the procedures given in section 4.3.5.1.

#### 4.3.5.3.2 Key Distribution for PMIP4

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

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



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

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

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 the home network (in which case the AAA broker does not exist) or in a visited CSN in which case there could be one or more AAA brokers between it and the HAAA server though it is not shown in Figure 4-9.

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

The following key distribution scheme applies:

The authenticator receives a set of mobility keys and other keys in the RADIUS Access-Accept or Diameter WDEA command message as a result of successful authentication. These include MN-HA-PMIP4, SPI-PMIP4, FA-RK, and HA-RK (with its SPI and lifetime). The keys are transported over RADIUS and are encrypted using the method defined in [42] section 3.5.

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

The HAAA distributes the MN-HA key, associated SPI, and the HA-RK key, if requested, to the HA using RADIUS Access-Accept or Diameter WMH4A command. In the case where the keys are transported over RADIUS, they are encrypted using the method defined in [42] section 3.5. For MN-HA, the HAAA sends the MN-HA-PMIP4 key to the HA when the SPI used in the MIP Registration Request is associated with PMIP4 MN-HA key (SPI = SPI-PMIP). A SPI value equal to SPI-PMIP4 indicates the MS is using PMIP, hence MN-HA-PMIP4 key is sent to the HA by the HAAA. The HA requests and uses these keys for verification of MN-HA AE and FA-HA AE according to the procedures described in section 4.8. Any new FA-HA key is derived in the HA from HA-RK according to the procedures given in section 4.3.5.1.

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

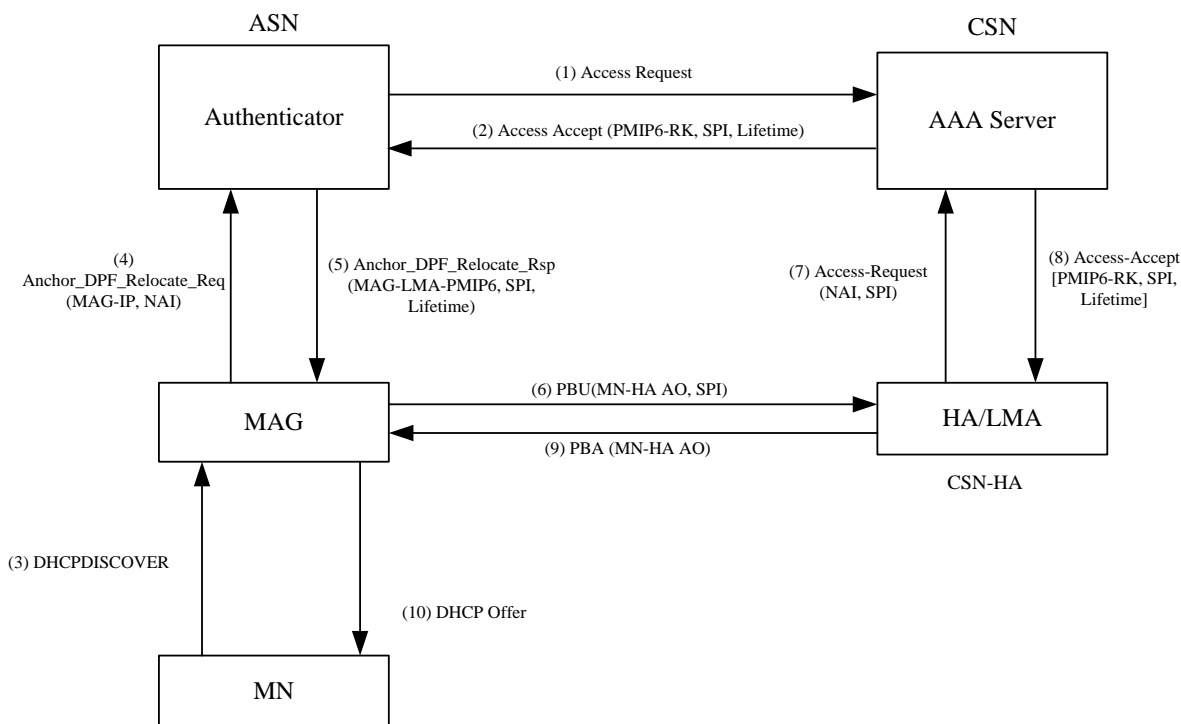
#### 4.3.5.3.3 Key Distribution for CMIP6

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

When the MIP6-Client in the MS commences MIP6 procedures it obtains the MN-HA-CMIP6 key. It uses this key to authenticate the Binding Update packet as defined by [71].

When the HA receives a Binding Update for which it does not have a security association, it sends an RADIUS Access-Request or Diameter WHA4R AND/OR WHA6R command to fetch the MN-HA key, from the HAAA. The HAAA provides the key to the HA in an RADIUS Access-Accept packet or Diameter WMHA6A command where in the case of RADIUS the Key is encrypted using the procedures defined in [42] section 3.5 and in the case of Diameter the keys are protected by the transport security (IPsec or TLS). The AAA messages MAY be transported between the HA and the HAAA via one or more AAA Brokers or proxies.

#### 4.3.5.3.4 Key Distribution for PMIP6



**Figure 4-10 – PMIP6 Key Distribution**

The MAG and the authenticator may be collocated or separated. Figure 4-10 illustrates the case when they are separated. The location of the LMA is shown such that it could be in the home network (in which case the AAA broker does not exist) or in a visited CSN in which case there could be one or more AAA brokers between it and the HAAA server though it is not shown in Figure 4-10.

The MAG requests the MAG-LMA-PMIP6 key along with the SPI and the lifetime from the Authenticator, when the MAG is ready to construct the PBU message toward the LMA.

The following key distribution scheme applies:

The Authenticator receives a set of mobility keys and other keys in the RADIUS Access-Accept message as a result of successful authentication. These include PMIP6-RK, PMIP6-RK-SPI and its lifetime. The keys are transported over RADIUS and are encrypted using the method defined in [42] section 3.5.

Before sending the PBU that includes in-band signaling security via AO, the MAG MUST obtain the MAG-LMA-PMIP6 key and its associated SPI and lifetime. If this is a relocation without re-authentication, the MAG obtains the MAG-LMA-PMIP6 key and its associated SPI and lifetime from the Authenticator using *Anchor\_DPF\_HO\_Req/Rsp* messages. The Authenticator derives MAG-LMA-PMIP6 key from the PMIP6-RK

according to the procedures given in section 4.3.5.1 and sets the associated SPI to the value of SPI-PMIP6, and the key lifetime to the remaining lifetime of the PMIP6/RK.

The HAAA distributes the PMIP6-RK key, SPI and the key lifetime, if requested, to the LMA using RADIUS Access-Accept. The keys are transported over RADIUS and are encrypted using the method defined in [42] section 3.5. After receiving the PMIP6-RK, the LMA derives the MAG-LMA-PMIP6 key according to the procedure given in section 4.3.5.1. The LMA uses the key for verification of MN-HA (MAG-LMA) Authentication Option according to the procedures described in [71]. If the same SPI was received at the LMA from a different MAG, the LMA SHALL generate a fresh MAG-LMA-PMIP6 key from the PMIP6-RK identified by that SPI.

#### 4.3.5.4 Key Lifetime

Lifetime of EMSK, MSK and derived keys (such as MIP-RK and PMIP6-RK) are the same.

MN-HA key lifetime is same as that of MIP-RK. The lifetime is transferred from Home AAA to Authenticator with Session-Timeout Attribute which is specified in section 5.3.2.373. When MN-HA key is transferred, its lifetime SHOULD be transferred as well.

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

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

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

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

MAG-LMA-PMIP6 lifetime inherits the remaining lifetime value of the PMIP6-RK lifetime.

#### 4.3.6 DHCP keys

DHCP messages between the DHCP relay and DHCP server are authenticated by the DHCP Authentication Suboption RFC using HMAC-SHA1 Algorithm as described in [65]. This algorithm requires that the DHCP relay and the DHCP server have a shared secret we call the DHCP-key. The DHCP-key is specific between each DHCP Relay and DHCP server. The DHCP keys are derived from the DHCP-RK. The DHCP-RK key generation is internal to the AAA server and is transported as necessary to the authenticator and DHCP server using AAA protocol. The DHCP Keys are derived from the DHCP-RK at the authenticator and at the DHCP server.

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

##### 4.3.6.1 Key Generation

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

The AAA server also generates a key identifier and associates it with the DHCP-RK. Key identifier is defined in [65] when using HMAC-SHA1 algorithm. Key identifier is unique within the scope of the single DHCP server. If several DHCP-RKs exist for a single DHCP server at the same time, they SHALL have different key identifiers. DHCP-RKs belonging to different DHCP servers may use the same key identifier. Apart from these constraints, the key identifier generation is internal to the AAA server. The size of the DHCP-RK is 160 bits. When Multiple DHCP Server is supported the AAA server SHALL also generate a key identifier and associates it with the DHCP-RK for each DHCP server.

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

$$\text{DHCP-key} = \text{HMAC-SHA1}(\text{DHCP-RK}, \text{"DHCP AUTH"} \mid \text{DHCP-Relay-IP} \mid \text{DHCP-Server-IP})$$

The size of the DHCP key is 160 bits.

#### 4.3.6.2 Key Distribution

In this section, DHCP key distribution is described. Table 4-5 describes where the DHCP keys are generated and where they are transported.

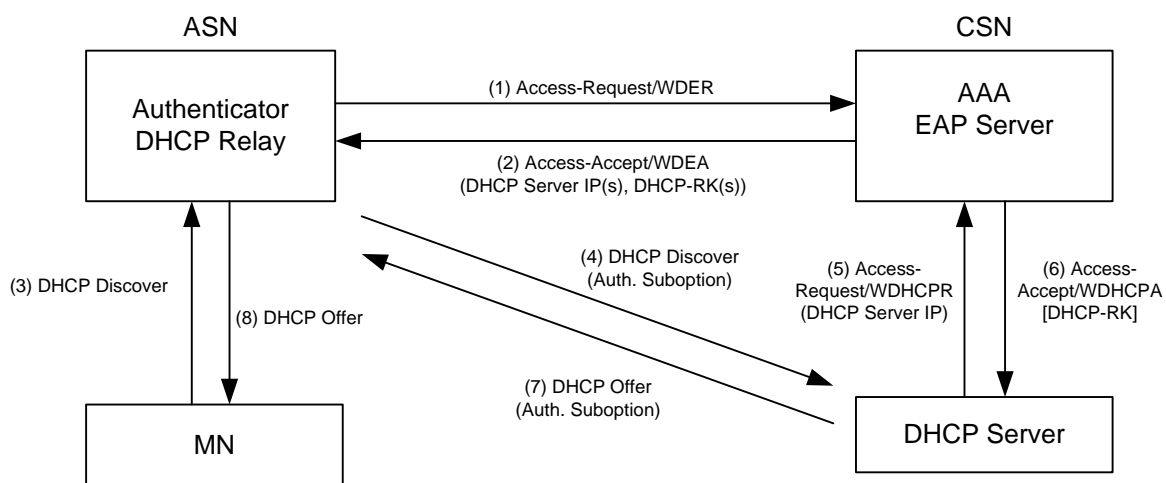
**Table 4-5 – DHCP Keys Generation and Usage**

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

The DHCP-RK keys are generated by the AAA server and are transported to the DHCP server and the Authenticator using the AAA protocol. The DHCP keys generated by the authenticator are transported to the DHCP relay via WiMAX specific R4 signaling. The DHCP - keys generated by the DHCP server are never transported outside of the DHCP server.

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

Figure 4-11 describes the distribution of DHCP keys for the case when the DHCP relay is collocated with authenticator:



**Figure 4-11 – Initial DHCP Key Distribution**

The authenticator receives a DHCP server address and the DHCP-RK in the RADIUS Access-Accept packet or Diameter WDEA command as a result of successful subscriber authentication. In case several DHCP-RKs associated with the DHCP server are available at the AAA server, the AAA server should include the DHCP-RK with the longest remaining lifetime in the RADIUS Access-Accept packet or the Diameter WDEA command.

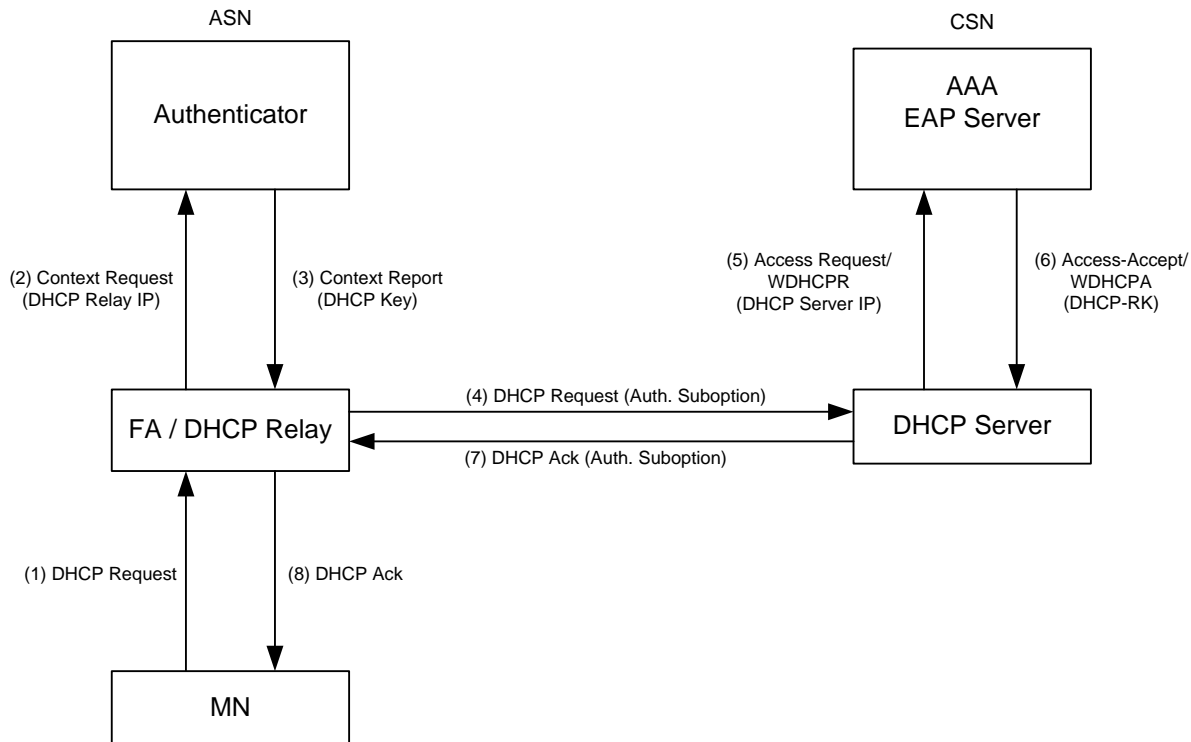


Besides DHCP-RK, the RADIUS Access-Accept packet or the Diameter WDEA command contains the lifetime and key identifier (DHCP-RK-Key-ID) of the DHCP-RK. The DHCP-RK is transported over AAA protocol and in the case of RADIUS is encrypted using the method defined in [42] section 3.5. When Diameter is used the DHCP-RK is protected by the Diameter transport security (IPsec or TLS). The AAA messages MAY be transported through zero or more AAA brokers or proxies. The keys are stored in the authenticator at the ASN.

At the time of DHCP procedures, the DHCP relay obtains the derived DHCP key from the Key-holder at the authenticator. The authenticator derives the DHCP key specific to the requesting DHCP relay from the DHCP-RK, as described in 4.3.6.1 and delivers the derived key, its lifetime and the key identifier associated with the DHCP-RK to the DHCP relay. DHCP relay uses the received DHCP key to compute the authentication suboption using HMAC-SHA1 as per [65] and includes the suboption populated with the Key ID and the HMAC result in the relayed DHCP message. When the DHCP server receives a message with authentication suboption, it searches for the corresponding DHCP key in its local cache by DHCP relay address and received key identifier. If the corresponding key is not found, the DHCP server derives a new DHCP key specific to this DHCP relay from the DHCP-RK associated with the Key ID. If a DHCP-RK is not found for the key identifier, the DHCP server acquires the DHCP-RK from the AAA server as described in section 4.8.2.1.2.3. Having acquired the DHCP-RK, the DHCP server derives the DHCP-key specific to the DHCP relay and stores it in its local cache. The lifetime of the derived key is limited to the lifetime of the DHCP-RK. DHCP server then uses the derived DHCP key to verify the authentication suboption as per [65]. In case the verification fails, or if AAA server responded with Access-Reject or a Diameter WDHCPA command with Result-Code AVP set to the “DIAMETER\_AUTHENTICATION\_REJECTED” failure result (as defined for the Diameter AAR command), the DHCP server SHALL drop the incoming message, as per [65].

The DHCP server SHALL provide the DHCP response message with the authentication suboption, as per [65].

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



**Figure 4-12 – DHCP Key Distribution when Authenticator and DHCP Relay are not collocated**

When the DHCP Relay intercepts a DHCP message from the MS and R3 is not secured (example – using IPsec), DHCP Relay SHALL add the authentication suboption to the message, as per [65] and use the HMAC-SHA1 algorithm. If the key corresponding to the DHCP server of the MS is not available at the DHCP Relay, the DHCP Relay will request a key from the authenticator by sending the *Context\_Req* message containing the DHCP Relay IP address TLV and an empty DHCP-Key TLV. The DHCP Relay address included in the *Context\_Req* message SHALL be the same address that the DHCP Relay will put into the giaddr field when relaying the DHCP message to the server. The authenticator will derive the necessary key, as described in 4.3.6.1 and deliver the derived key, its lifetime and the key identifier associated with the DHCP-RK to the DHCP Relay in DHCP Relay Info subTLV of the *Context\_Rpt* message. Having acquired the DHCP key, the DHCP Relay proceeds as described above in the scenario when the DHCP Relay and authenticator are collocated.

**Table 4.3-1 – Context\_Req from DHCP Relay to Authenticator**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Set to indicate retrieval of DHCP-Relay-Info.
MS Info	5.3.2.103	M	
>DHCP Relay Info	5.3.2.56	M	Information about the DHCP Relay
>>DHCP Relay Address	5.3.2.55	M	DHCP Relay IP address for which the key is requested.

**Table 4.3-2 – Context\_Rpt from Authenticator to DHCP Relay**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Request Success or request failure or partial response.
Context Purpose Indicator	5.3.2.36	M	Set to indicate retrieval of DHCP-Relay-Info.
MS Info	5.3.2.103	M	
>DHCP Relay Info	5.3.2.56	M	Information about the DHCP Relay
>>DHCP Relay Address	5.3.2.55	M	DHCP Relay IP address for which the key is requested.
>>DHCP Key	5.3.2.51	M	Key used to calculate and authenticate messages between the DHCP relay and DHCP server.
>>DHCP Key ID	5.3.2.52	M	Key ID associated with the key used to compute authentication suboption
>>DHCP Key Lifetime	5.3.2.53	M	The remaining lifetime in seconds of the DHCP key.
>>DHCP Server Address	5.3.2.57	O	The IP address of the DHCP Server.

## 4.4 Authentication, Authorization and Accounting

### 4.4.1 Network Access Authentication and Authorization

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

Network Access Authentication and Authorization is performed using RADIUS and Diameter AAA protocols. In the case of RADIUS the protocols used in are based on the IETF RADIUS protocols as embodied by the following RFCs:

- RFC 2865 [37]
- RFC 3579 [52]

In the case of Diameter, Network Access Authentication and Authorization utilizes a WiMAX specific application defined by this specification that is based on the IETF Diameter EAP Application RFC4072 [66].

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

**Table 4-6 – 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.
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.

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

After successful network access authentication, the HAAA delivers authorization attributes to the NAS. Since the design goal is to reduce the number of AAA transactions, the HAAA delivers all possible attributes to the NAS. For example, the HAAA will deliver attributes required for PMIP4 operations without knowing whether PMIP4 will be invoked. As part of the MS authorization attributes, HAAA decides for the MS-Certified-Feature-List-For-GW and MS-Certified-Feature-List-For-BS based on the MS certified capability and end-to-end network capability.

#### 4.4.1.1 Network Access Authentication Model

The HNSP always performs authentication to verify the subscriber credential. While doing so, the HNSP MAY also require verification of device credential. HNSP policy determines when to perform the latter (e.g., during initial network entry, or also for each re-authentication, etc.) If the subscriber and device credentials are distinct and both need to be authenticated, either a tunneling EAP method (e.g., EAP-TTLS) or credential combining (see section 4.4.1.4.1.1.2) is used.

Each EAP authentication involves executing an EAP method (e.g., EAP-TLS, EAP-TTLS, EAP-AKA, etc.). The EAP method and the associated credential selection is a deployment decision. Mandatory to implement methods are described in Section 4.4.1.2. The MS and the EAP authentication server uses [56] EAP method negotiation to dynamically select a method during network access authentication.

#### 4.4.1.2 EAP Methods

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

For user authentication, MS SHALL support at least one of EAP-AKA [16] or EAP-TTLS [18].

For user authentication, H-NSP SHALL support at least one of EAP-AKA [16] or EAP-TTLS [18] and SHOULD support both.

For those EAP methods that utilize server certificates, the MS SHOULD check the revocation status of AAA server's X.509 certificate at the time of network access authentication. MS SHOULD use and HAAA SHALL support light-weight profile [86] of OCSP [59] over EAP-TLS [17] by means of TLS extensions [82].

##### 4.4.1.2.1 EAP-TLS

Whether or not to perform Device Authentication using EAP-TLS is up to the operator's 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 fragmentation function described in the section 3.3 of [17]. The MTU size of EAP-TLS fragmentation SHALL be 1400 bytes to avoid unnecessary additional fragmentation/unnecessary additional 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:

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

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

The EAP-TLS client in MS MUST support at least one, and the EAP-TLS Server (HAAA server) MUST as a minimum support all of the following cryptographic suites:

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

The AAA server SHALL parse the x.509 certificate sent to it by the MS during EAP-TLS. The MAC address and Model SHALL be extracted from the X520CommonName RDN. The MAC SHALL be compared with the MAC address in the Calling-Station-Id of the RADIUS Access-Request packet or Diameter WDER command. If they do not match the authentication SHALL be rejected.

If the MAC address matching is successful, the EAP method executes to completion. If the EAP method terminates with EAP-Failure, the MS, BS, and the authenticator SHALL perform the disconnection procedure as defined in [11]. Furthermore, if the MS received network rejection information via EAP Notification, then the MS SHALL act according to the section 4.5.1.3. If the EAP method is completed with an EAP-Success, the MS SHALL parse the server's X.509 certificate sent to it by the AAA during EAP-TLS. The domain name of service provider SHALL be extracted from the X520CommonName RDN of the server certificate. The extracted domain name SHALL be compared against the configured list of realms, associated with home operator, for a particular subscription using the matching rules associated with this list (if available) or the realm in Outer-Identity. In case of the mismatch, the MS SHALL reject the connection, unless the MS is instructed by the user or pre-configured to proceed despite the mismatch. Regardless of the match or mismatch, the MS continues the EAP session with the NSP that sent the certificate.

If the EAP session is completed successfully (i.e. the MS receives SA\_TEK\_CHL with a valid CMAC), the MS SHALL act depending on the match or the mismatch. In case of the match, when receiving 802.16 SA\_TEK\_Challenge message from the BS, the MS SHALL respond with SA\_TEK\_Request in order to continue the connection procedure. On the other hand, in case of the mismatch, the MS SHALL reject the connection, unless the MS is instructed by the user or pre-configured to proceed despite the mismatch.

According to the default rule: A match is achieved if the Outer-Identity realm and service provider domain are either the same or one is a sub-domain of the other.

Examples:

Outer-Identity = MAC@xyz.com and service provider domain name = abc.xyz.com will be a match.

Outer-Identity = MAC@xyz.com and service provider domain name = xxx.abc.xyz.com will be a match.

Outer-Identity = MAC@abc.xyz.com and service provider domain name = ABC.XYZ.com will be a match.

Outer-Identity = MAC@bbb.xyz.com and service provider domain name = xyz.com will be a match.

Outer-Identity = MAC@bbb.xyz and service provider domain name = bbb.xyz.com will NOT be a match.

#### **4.4.1.2.2 EAP-AKA**

When EAP-AKA is used for user authentication, MS SHALL support the full authentication procedure described in [16]. When EAP-AKA is used, the subscriber credential SHALL be used in generation of authentication vectors defined in [16]. 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 [18] and MS-CHAPv2 [19] 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 fragmentation SHALL be 1400 bytes to avoid unnecessary 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 [18]. Note that [18] 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:

$$\text{MSK}(0,63) = \text{TLS-PRF-64}(\text{SecurityParameter.master secret}, \text{"tls keying material"}, \text{random}).$$

$$\text{EMSK}(0,63) = \text{second 64 octets of: TLS-PRF-128}(\text{SecurityParameter.master secret}, \text{"tls keying material"}, \text{random}).$$

Where: random = SecurityParameters.client\_random || SecurityParameters.server\_random.

The EAP-TTLS client in MS MUST support at least one, and the EAP-TTLS Server (HAAA server) MUST as a minimum support all of the following cryptographic suites:

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

The MS SHALL parse the server's X.509 certificate sent to it by the AAA during EAP-TTLS. The domain name of service provider SHALL be extracted from the X520CommonName RDN of the server certificate. The extracted domain name SHALL be compared against the configured list of realms, associated with home operator, for a particular subscription using the matching rules associated with this list (if available) or the realm in Outer-Identity. If they do not match, the MS SHOULD notify the user and MS SHOULD reject authentication unless the MS is instructed by the user or configured to proceed despite the mismatch.

According to the default rule: A match is achieved if the Outer-Identity realm and service provider domain are either the same or one is a sub-domain of the other.

Examples:

Outer-Identity = MAC@xyz.com and service provider domain name = abc.xyz.com will be a match.

Outer-Identity = MAC@xyz.com and service provider domain name = xxx.abc.xyz.com will be a match.

Outer-Identity = MAC@abc.xyz.com and service provider domain name = ABC.XYZ.com will be a match.

Outer-Identity = MAC@bbb.xyz.com and service provider domain name = xyz.com will be a match.

Outer-Identity = MAC@bbb.xyz and service provider domain name = bbb.xyz.com will NOT be a match.

The AAA server SHALL parse the x.509 certificate if sent to it by the MS during EAP-TTLS. The MAC address and Model SHALL be extracted from the X520CommonName RDN. The MAC SHALL be compared with the MAC address in the Calling-Station-Id of the RADIUS Access-Request packet or Diameter WDER command. If they do not match, the authentication SHALL be rejected.

#### 4.4.1.3 Network Access Identifier

The Network Access Identifier (NAI) SHALL conform to [68]. 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 defined in section 4.4.1.3.1. 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 packet or the Diameter WDER command. The Outer-Identity at initial network entry is also used to populate the MS NAI TLV in the MS Authorization Context TLV in the MS Info TLV. Even though the Outer-Identity may change across subsequent re-authentications, the MS NAI values SHALL stay fixed to the initial one until network exit.

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 as recommended by [64] and section 5.1 of [40]. The AAA User-Name attribute is set to this value in the RADIUS Access-Request or Diameter WDER command. 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:

<routing realms><WiMAX decoration><username>@<realm>Where:

routing realms: Optionally used. The use of routing realm is described in [68]. Example: hnspl.com!joe@vnsp.com

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 [68]. The name must be alphanumeric with no spaces.

Example: {fm=1|xm=3}joe@hnspl.com

The MS SHALL decorate the NAI with the CRN. The NAI decoration SHALL be based on AVP definition as per Table 4-7.

Currently the following AVPs are defined:

**Table 4-7 – WiMAX decoration AVP definitions**

AVP	Values	Comments	WMF Specification
sm	1 (for over-the-air provisioning) 2 (for emergency network entry)	Service Mode indication for over-the-air provisioning and emergency services	For value 1: T33-103-R015v04-OTA-General [6] For value 2: T33-102-R015v02-_Emergency-Services [5]
crn	Certification Registration Number (CRN) expressed in ASCII HEX assigned to the MS as part of the WiMAX Forum Certification Program.	Carries the Certification Registration Number for Certification Version signaling (CVS)	This document.

All other AVPs and Values not listed in Table XX are reserved.

username: The user name is as defined by the EAP method with the following caveat. 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 [68]. When the realm is not specified, the preceding ‘@’ SHALL be omitted as well. Example: joe

When the NAI is generated for CMIP or PMIP, it SHALL NOT include any decoration (routing realms or WiMAX decoration). The NAI is formatted by the username@homerealm or username when home realm is not available. For example: “joe” or “joe@hnspl.com” are valid Mobile IP NAIs generated by WiMAX. When there is no routing realm in the NAI, home realm is the realm following the ‘@’ symbol. Otherwise, home realm is the right-most realm in the routing realms part of the NAI.

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 a RADIUS Access-Request or Diameter WDER command 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 a RADIUS Access-Reject or Diameter WDEA with Result-Code AVP indicating failure and 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 same username and home realm (if available) used in the EAP-Response Identity of the initial network access authentication.
- Similarly, in the case of PMIP, the PMIP4 client SHALL construct the NAI extension as above by using the PMIP-Authenticated-Network-Identity if received from the AAA, otherwise the NAI SHALL be constructed by using the same username and home realm (if available) used in the EAP-Response Identity of the initial network access authentication.
- If there is an ongoing MIP session, then the MS (or PMIP client) SHALL continue to use the same NAI in the MIP NAI extension that it has been using.
- In case of MIP6, the username and HCSN realm is carried in identifier option ([71]).

#### **4.4.1.4 Detailed Impact on Functional Entities**

##### **4.4.1.4.1 MS Requirements**

###### **4.4.1.4.1.1 General Requirements**

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

ASN selects Single EAP during SBC negotiation.

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

The authentication procedure MAY be for authenticating only subscriber credential, or both subscriber and device credentials. HNSP has the flexibility with respect to when to authenticate the device credential. This policy is assumed to be known to the MS. Details of how MS learns this policy is outside the scope of this specification.

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

In response to EAP-Request Identity, the MS SHALL set the realm part of the NAI to be the FQDN of the HCSN. This is where the EAP authentication server resides. If network routing is being utilized, the MS MUST ensure that the route specified in the NAI terminates at the HCSN. The length of this NAI MUST NOT exceed 253 octets.

After sending the EAP-Response Identity, the MS receives EAP-Request EAP-method suggesting the method to use for performing the authentication. If the MS does not agree with the selected method then the MS SHALL respond with an EAP-Response NAK suggesting its preferred EAP method to use for that authentication. Otherwise, the MS starts executing the EAP-method. If the authentication fails, the MS SHALL be denied network entry.

After successful completion of the authentication, the MS SHALL compute the keys required for PKMv2 using the MSK. The MS SHALL use the EMSK to compute other application keys (see section 4.3.1).



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

Duplicate detection of EAP messages is limited to only one EAP conversation (which ends with an EAP Success or EAP Failure message). MS SHALL NOT expect the EAP Identifier field of the message that initiates another EAP conversation (i.e., re-authentication) to be different than that of the EAP message that concluded the previous conversation. Coincidentally the two values may be the same at times, and MS SHALL NOT treat the new message as duplicate in such cases.

If an X.509 certificate is used for authenticating the HAAA along with the OCSP procedure (e.g., as in EAP-TLS) and the MS encounters a new OCSP responder, the MS SHOULD download the OCSP CRL using HTTP after the network access is granted. If the MS discovers that OCSP responder's certificate is listed as revoked in the CRL, then the MS SHALL regard the network access authentication procedure as failed and initiate network exit procedure. If the MS encounters a known OCSP responder, it SHOULD perform the check again if a pre-configured amount of time has elapsed since the last check on the responder's certificate.

#### **4.4.1.4.1.1.1 Authenticating Subscriber Credential**

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

If an EAP method that relies on availability of subscriber credentials on the MS (e.g., EAP-TTLS with MSCHAPv2) fails, the MS SHALL retry authentication for a finite number of times (e.g., 3). If the successful authentication is not achieved after the last attempt, the MS SHOULD send EAP-Response NAK in response to the EAP method requested by the network and suggest its preferred EAP method as EAP-TLS. This allows the MS to enter the network for treatment using X.509 device certificate based authentication (i.e., without the subscriber credentials such as username and password). Treatment of the MS is beyond the scope of this specification. When the MS is allowed to enter the network under this circumstance, the network SHOULD provide limited access service to the MS.

#### **4.4.1.4.1.1.2 Authenticating Subscriber and Device Credentials**

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

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

Combined\_identifier = MAC\_address | “-” | user\_ID

Combined\_PSK = truncate(HMAC-SHA256(PSK\_device, PSK\_user), N)

MAC\_address is the 48-bit IEEE 802.16 MAC address printed as 6 2-digit hexadecimals delineated by hyphens (“-“, ASCII x2D). For example: “00-11-22-33-44-55”. User\_ID is the identifier of the PSK\_user. For example: “joe@isp1.com”. The example combined identifier would be “00-11-22-33-44-55-joe@isp1.com”.

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

Once generated, Combined\_identifier and Combined\_PSK can be used with a PSK-based authentication method executed between the MS and the HCSN. Successful execution of the method indicates both the subscriber and the device are authenticated.

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

Some tunneled EAP methods (e.g., EAP-TTLSv0) are susceptible to man-in-the-middle attacks when one of the end-point cannot verify that both the inner and the outer method are executed by the same entity. One way to

prevent such a threat is to cryptographically bind the inner and the outer authentication methods. Note this is not supported by all tunneled methods (such as EAP-TTLSv0). Another is to ensure that both the MS and the HAAA configurations are always in-synch with respect to when to engage tunneled EAP methods as opposed to using the inner method only. Deployments SHOULD use one of these remedies or their equivalents when using at-risk EAP methods.

#### **4.4.1.4.2 NAS Requirements**

The NAS SHALL support RADIUS and MAY support Diameter AAA protocols. A NAS that supports Diameter based Network Access Authentication SHALL conform to RFC3588 [54] and advertise support for the “WiMAX Network Access Authentication and Authorization Diameter Application” (see section 5.5.1.1).

##### **4.4.1.4.2.1 General Requirements**

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

Network access authentication phase SHALL commence upon receiving an EAP-Response-Identity. Otherwise, the NAS SHALL reject the session and not allow the MS network access.

The NAS SHALL act as an EAP pass-through ([56]) and route the AAA messages according to routing information in the NAI. If there is no routing information (i.e., realm is missing), then it is up to the implementation/deployment to decide if and how the AAA messages are routed. The NAS receives an MSK at the end of successful authentication.

While acting as a pass-through authenticator, if the NAS receives an EAP-Request Identity in a AAA message before receiving EAP-Success or EAP-Failure indication, the NAS SHALL terminate the authentication procedure and send an EAP-Request Identity to the MS.

Upon receiving an RADIUS Access-Reject or Diameter WDEA with EAP-Failure indication, the NAS SHALL deny the MS network access.

Upon receiving a RADIUS Access-Accept or Diameter WDEA with EAP-Success indication, the NAS SHALL save the MSK and follow the procedures as specified in section 4.3.4. The NAS SHALL bind the state for the MS to the R6 path identifier (for IP-CS) or the MAC address for (Ethernet-CS). This binding is used to verify that a particular traffic flow is coming from a specific device.

##### **4.4.1.4.2.2 RADIUS Message Processing**

###### **4.4.1.4.2.2.1 Initial Access-Request**

The NAS SHALL send an Access-Request as triggered by the EAP process to initiate authentication. The attributes for the Access-Request are listed in Stage 3 Annex – Prepaid Accounting and section 5.3.2.373.

The NAS SHALL set the EAP-Message attribute to the value received in the EAP-Response/Identity. The NAS SHALL follow the procedures defined in [52] for processing the RADIUS messages carrying EAP data. This includes setting the value of the Message-Authenticator attribute.

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

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

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

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

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

If the NAS supports fixed and nomadic access, it SHALL include either the serving BS-ID or the serving BS Location attribute, or both, in the RADIUS Access-Request message.

**4.4.1.4.2.2 Responding to RADIUS Challenge**

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

If the NAS receives an EAP-Request Identity in a RADIUS Access-Challenge message before receiving EAP-Success or EAP-Failure indication, the NAS SHALL terminate the authentication procedure and send an EAP-Request Identity to the MS.

**4.4.1.4.2.3 NAS Receives Access-Accept from HAAA**

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

As per [52], the NAS SHALL validate the Message-Authenticator (80) attribute. The NAS SHALL silently discard the Access-Accept packet if the Message-Authenticator attribute is not present in the packet or if the computed Message Authenticator does not match the value received in the packet.

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

The NAS receives a set of attributes for Mobile IP procedures which the NAS stores against the session context. See PMIP and CMIP sections in 4.8. In particular, the NAS may receive two sets of HA attributes, one allocated by VAAA, another allocated by HAAA for dynamic HA allocation procedure. The NAS SHALL store these two sets of HA attributes to be later used for dynamic HA resolution as specified in section 4.8. Each set of HA attribute includes HA address, HA-RK, HA-RK SPI and HA-RK lifetime. If HA in visited network is selected, the HA attributes allocated by VAAA are applied; likewise, if HA in home network is selected, the HA attributes allocated by HAAA are applied.

The NAS SHALL store the received Framed-IPv6-Prefix attribute(s).

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

The NAS SHALL store the first Class attribute if received in the Access-Accept associated with the network access authentication.

The NAS SHALL store the MAC address of the MS.

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

The NAS SHALL store the PMIP-Authenticated-Network-Identity received in the Access-Accept. If the PMIP-Authenticated-Network-Identity attribute is received, this value SHALL be used by the PMIP client to set the PMIP NAI.

The NAS SHALL store the MS-Certified-Feature-List-For-GW and MS-Certified-Feature-List-For-BS received in the Access-Accept as part of MS Context. This attribute list is used to limit the MS to the certified feature list only.

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

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

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

If the NAS supports fixed and nomadic access then it SHALL store the Mobility Access Classifier if received in the Access-Accept. If the NAS does not support fixed and nomadic access then it SHALL ignore the Mobility access Classifier if received in the Access-Accept.

1 If the NAS supports only fixed access (due to regulatory restrictions for example), then any mobility access  
2 classifier other than fixed received in the Access-Accept may be treated as a fixed mobility access classifier or  
3 denied service based on the NAS local policy.

4 If the NAS supports only fixed and nomadic access, then a mobility access classifier of Mobile received in the  
5 Access-Accept may be treated as a nomadic access classifier or denied service based on the NAS local policy.

6 The NAS SHOULD initiate MS network exit for any MS using the same MAC address as the one that is newly  
7 authenticated by the Access-Accept message received from the HAAA, unless the MS already residing in the  
8 network performed device authentication during initial network entry and has an authenticated MAC address, but  
9 the newly authenticated MS did not perform device authentication (indicated by the value of the MS-Authenticated  
10 attribute, if present in the Access-Accept message from the HAAA).

11 The MS trying the new network entry, if not device-authenticated, should be considered a misbehaving device in  
12 case there is an already existing WiMAX session with an authenticated MAC address. If for the new network entry  
13 the MS indicates an emergency network entry, this should be taken into account. However, the actual policy for how  
14 to deal with emergency network entry in this situation is up to the CSN operator's policy and depends on the local  
15 regulatory environment.

#### 16 **4.4.1.4.2.2.4 NAS Receives Final Access-Reject**

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

18 The NAS SHALL validate the Message-Authenticator (80) attribute as per [52]. The NAS SHALL silently discard  
19 the Access-Reject packet if the Message-Authenticator attribute is not present or the computed Message  
20 Authenticator does not match the value received in the Access-Reject packet.

#### 21 **4.4.1.4.2.3 Diameter Message Processing**

##### 22 **4.4.1.4.2.3.1 DER**

23 The NAS SHALL send a WDER command as triggered by the EAP process to initiate authentication. The NAS  
24 SHALL follow the procedures defined in RFC4072 [66] with the following clarification:

- 25 • The NAS SHALL include the WiMAX-Capability AVP as describe in section 5.5.2.1.
- 26 • The NAS SHALL set the EAP-Payload attribute to the value received in the EAP-Response/Identity from the  
27 MS,
- 28 • The NAS SHALL set the value of the Calling-Station-ID AVP to the MS's MAC address.
- 29 • If the NAS supports CUI and it requires CUI to be delivered by the HAAA, then the NAS SHALL include the  
30 CUI attribute in the WDER command and SHALL set its value to a single ASCII NUL character.
- 31 • The NAS SHOULD forward the WDER packet to the VAAA in the visited CSN using the routing decoration of  
32 the NAI, if any.
- 33 • During EAP authentication process when the NAS acts in pass through mode, the NAS MUST validate the EAP  
34 header fields as specified in RFC4072 [66].
- 35 • If the NAS supports fixed and nomadic access, it SHALL include either the serving BS-ID or the serving BS  
36 Location AVP, or both, in the Diameter WDER command.

##### 37 **4.4.1.4.2.3.2 DEA**

38 EAP authentication requires multiple AAA transactions, that is, the NAS will receive WDEA command with Result-  
39 Code AVP set to "DIAMETER\_MULTI\_ROUND\_AUTH". Processing of these messages conform to the  
40 RFC4072 [66].

41 During EAP processing the NAS acts in passthrough mode and MUST validate the EAP header fields contained in  
42 the EAP-Payload AVP as defined by RFC4072 [66].

43 The NAS SHALL receive a final WDEA command with Result-Code AVP indicating success or failure and the  
44 EAP-Payload containing EAP-Success or EAP-Failure.

- 1 If the WDEA command indicates failure the NAS SHALL forward the contents of the EAP message to the MS and  
2 disallow the MS WiMAX Network Access.
- 3 If the final WDEA command does not contain the EAP-Master-Session-Key AVP, then the NAS MUST treat the  
4 response as a rejection and disallow WiMAX network access.
- 5 If the NAS required the inclusion of the CUI attribute and the final WDEA command does not contain the CUI  
6 attribute then the NAS MUST treat the response as a rejection and disallow WiMAX network access.
- 7 If the WDEA command includes all the needed attributes and indicates success, the NAS SHALL forward the  
8 contents of the EAP message to the MS. This marks the start of the WiMAX session for the MS.
- 9 The NAS SHALL store the MSK key. The MSK key is used for computing the AK used for securing the 802.16 air  
10 interface.
- 11 If the NAS received a set of attributes for Mobile IP procedures it stores against the session context. See PMIP and  
12 CMIP sections in 4.8. In particular, the NAS MAY receive two sets of HA attributes, one allocated by VAAA,  
13 another allocated by HAAA for dynamic HA allocation procedure. The NAS SHALL store these two sets of HA  
14 attributes to be later used for dynamic HA resolution as specified in section 4.8. One set of HA attribute includes  
15 HA address, HA-RK, HA-RK SPI and HA-RK lifetime. If HA in visited network is selected, the HA attribute  
16 allocated by VAAA is applied; otherwise, if HA in home network is selected, the HA attribute allocated by HAAA  
17 is applied.
- 18 The NAS SHALL store the received Framed-IPv6-Prefix attribute(s).
- 19 The NAS SHALL store the CUI received. The CUI SHALL be sent in each Diameter Accounting-Request  
20 command.
- 21 The NAS SHALL store the first Class attribute if received in the Diameter WDEA associated with the network  
22 access authentication.
- 23 The NAS SHALL store the WiMAX-Session-Id attribute received in the WDEA command. The WiMAX-Session-  
24 Id SHALL be used in all subsequent WDER commands. The WiMAX-Session-Id is also sent in the Diameter  
25 Accounting commands. Note that the WiMAX-Session-Id is different than the Diameter Session-ID. The Diameter  
26 Session-Id is established by the NAS and is unique to the NAS/AAA. Whereas the WiMAX-Session-Id is  
27 established for the WiMAX network access authentication session.
- 28 If received, the NAS SHALL store the PMIP-Authenticated-Network-Identity received in the Access-Accept. If the  
29 PMIP-Authenticated-Network-Identity attribute is received, this value SHALL also be used by the PMIP client to  
30 set the PMIP NAI.
- 31 If the NAS receives Prepaid attributes, it SHALL process them as per section 4.4.3 and Stage 3 Annex – Prepaid  
32 Accounting.
- 33 If the NAS receives Filter and Tunneling attributes, it SHALL process them as per section 4.4.3.5.
- 34 If the NAS supports fixed and nomadic access, then it SHALL store the Mobility access Classifier if received in the  
35 Diameter WDEA. If the NAS does not support fixed and nomadic access then it SHALL ignore the Mobility access  
36 Classifier if received in the WDEA command.
- 37 If the NAS supports only fixed access (due to regulatory restrictions for example), then any mobility access  
38 classifier other than fixed received in the Diameter WDEA command may be treated as a fixed mobility access  
39 classifier or denied service based on the NAS local policy.
- 40 If the NAS supports only fixed and nomadic access, then a mobility access classifier of Mobile received in the  
41 Diameter WDEA command may be treated as a nomadic access classifier or denied service based on the NAS local  
42 policy.
- 43 The NAS SHOULD initiate MS network exit for any MS using the same MAC address as the one that is newly  
44 authenticated by the WDEA command received from the HAAA, unless the MS already residing in the network  
45 performed device authentication during initial network entry and has an authenticated MAC address, but the newly  
46 authenticated MS did not perform device authentication (indicated by the value of the MS-Authenticated AVP, if  
47 present in the WDEA command from the HAAA).

The MS trying the new network entry, if not device-authenticated, should be considered a misbehaving device in case there is an already existing WiMAX session with an authenticated MAC address. If for the new network entry the MS indicates an emergency network entry, this should be taken into account. However, the actual policy for how to deal with emergency network entry in this situation is up to the CSN operator's policy and depends on the local regulatory environment.

#### **4.4.1.4.2.3.3 Termination of Session**

When the NAS terminates a session the NAS SHALL conform to Diameter [54] and send a WiMAX Session Termination Request (WSTR) command indicating that the session for the mobile has terminated.

The WSTR command SHALL be sent anytime the session is terminated irrespective of how it was terminated. Note that the NAS MUST also send a WSTR for a session that was authorized but that has not started.

The NAS SHALL receive a WiMAX Session Termination Answer (WSTA) command from the HAAA.

The AVPs for the WSTA/WSTR are given in section 5.5.

#### **4.4.1.4.3 Visited CSN AAA Requirements**

The Visited CSN plays the role of a AAA proxy. To choose the target VCSN the VCSN can be statically configured at the ASN. Alternatively, the Routing Realm used in the User-Name (NAI) attribute of the AAA message can contain the FQDN of the selected VCSN.

The Visited CSN AAA SHALL support RADIUS and MAY support Diameter AAA protocols. A Visited CSN AAA that supports Diameter based Network Access Authentication SHALL conform to RFC3588 [54] and advertise support for the “WiMAX Network Access Authentication and Authorization Diameter Application” (see section 5.5.1.1). The VAAA MAY act as a Diameter Proxy.

##### **4.4.1.4.3.1 VCSN Acting as AAA Proxy**

During all AAA interaction the VCSN AAA server acts as a RADIUS or Diameter proxy transporting AAA messages between the ASN and the HCSN.

During proxy operation the AAA Proxy SHALL validate all RADIUS packets containing EAP messages as per [52]. Similarly, a Diameter AAA Proxy SHALL conform to RFC4072 [66]. In the case of RADIUS, if the packets received are invalid the RADIUS proxy SHALL discard the packet.

During routing operations the VCSN SHALL process the NAI found in the User-Name attribute as specified by [68] and route the RADIUS packets accordingly. When using Diameter routing is performed based on RFC3588 [54]. VAAA MAY need to remember the routing decoration of the NAI if it chooses to send the subsequent Access-Request or the Accounting messages for Mobile IP in the same route as the AAA messages used for network access authentication. When the VAAA receives the AAA messages from the vHA/vLMA, the NAI may not include the decoration part. VAAA MAY decorate such NAI with what it remembers from network access authentication procedure.

To support dynamic HA allocation in VCSN, the VAAA MAY include a vHA-IP-MIP4 attribute and/or a vHA-IP-MIP6 attribute in the first RADIUS Access-Request packet or the Diameter WDER command of initial authentication session to be forwarded to HAAA, if local network policy allows. These attributes contain IPv4 address and IPv6 address of the local HA that will process the MIP signaling messages, if visited network HA is used.

The VAAA SHALL NOT include vHA-IP-MIP4 and/or vHA-IP-MIP6 attributes in either RADIUS Access-Request packets or Diameter WDER command if EAP authentication involves multiple rounds of Access-Request/Access-Challenge or WDEA/TBD exchange. The VAAA SHALL NOT include vHA-IP-MIP4 and/or vHA-IP-MIP6 attributes in Access-Request during EAP re-authentication.

If the same vHA-IP-MIP4 attribute is echoed by HAAA in RADIUS Access-Accept or the Diameter WDEA command, possibly in addition to the hHA-IP-MIP4, hHA-IP-MIP6, hHA-RK-KEY, hHA-RK-SPI, and hHA-RK-Lifetime attributes assigned by the HAAA, the VAAA SHALL additionally include vHA-RK-KEY, vHA-RK-SPI and vHA-RK-Lifetime attributes in the RADIUS Access-Accept or Diameter WDEA command to be forwarded to

NAS. The generation of HA-RK, SPI and its lifetime is specified in section 4.3.5.1. When generating the vHA-RK-SPI, the VAAA SHALL avoid collisions with any known HA-RK-SPI associated with the vHA.

To support dynamic HA allocation in VCSN, dynamic DHCP server allocation SHALL be supported in VCSN for the DHCP Relay mode. The VAAA MAY include the vDHCPv4 and/or vDHCPv6-server attribute in the AAA Access-Request to be forwarded to HAAA, if local network policy allows. These contain the local DHCP server attributes that will be used by the visited HA.

If the same vDHCPv4-server attribute is echoed by HAAA in AAA RADIUS Access-Accept or Diameter WDEA, the VAAA SHALL additionally include the vDHCP-RK, vDHCP-RK-Key-ID and vDHCP-RK-Lifetime attributes in the RADIUS Access-Accept packet or the Diameter WDEA command to be forwarded to NAS. The generation of DHCP-RK, ID and its lifetime is specified in section 4.3.6.1.

The VAAA MAY include the Visited-Framed-Interface-Id and the Visited-Framed-IPv6-Prefix attribute in the RADIUS Access-Request packet or Diameter WDER command to be forwarded to h-AAA, if local network policy allows.

The HAAA may decide based on local network policies to remove or echo the Visited-Framed-Interface-Id and the Visited-Framed-IPv6-Prefix attribute in the RADIUS Access-Accept packet or Diameter WDEA command. The final RADIUS Access-Accept packet or Diameter WDEA may include the following attributes: Framed-Interface-Id and/or Visited-Framed-Interface-Id, and Framed-IPv6-Prefix and/or Visited-Framed-IPv6-prefix.

#### **4.4.1.4.4 Home CSN AAA Requirements**

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

The HAAA plays the role of the EAP authentication server.

The Home CSN AAA SHALL support RADIUS and MAY support Diameter AAA protocols. A Home CSN AAA that supports Diameter based Network Access Authentication SHALL conform to RFC3588 [54] and advertise support for the “WiMAX Network Access Authentication and Authorization Diameter Application” (see section 5.5.1.1).

Network access authentication starts when the HAAA receives a RADIUS Access-Request packet containing an EAP-Message payload or a Diameter WDER command containing an EAP-Payload AVP which is set to the MS EAP-Response/Identity. This message is sent from the NAS in the ASN to the HAAA server in the HCSN via the AAA Proxy in the VCSN and perhaps one or more AAA brokers. In the case of RADIUS, the AAA packets exchanged between the NAS and the HAAA are Access-Request, Access-Accept, Access-Reject and Access-Challenge (see Table 5-5). These messages comply with the RADIUS RFCs and the additional requirements given in this specification. In the case of Diameter, the AAA commands exchanged are based on the WiMAX Network Access Authentication and Authorization Diameter application which is based on Diameter EAP Application (RFC4072 [66]).

The MSK and EMSK that result from network access authentication will be used to further derive other keys used in other procedures. The MSK is required and SHALL be transported to the NAS using the MSK vendor attribute in the case of RADIUS and the EAP-Master-Session-Key AVP in the case of Diameter. The EMSK is used to derive application keys and never leaves the AAA.

The HAAA also derives certain keys and information required for subsequent procedures. The information is described below. Some of the data is transported to the NAS (and entities along the route) using RADIUS Access-Accept packet or Diameter WDEA command and some of the information is cached and used for subsequent procedures such as mobility authentication procedures.

The HAAA SHALL verify as part of network access authentication that the MS MAC address received in Calling-Station-ID from the Authenticator does not match the MS MAC address of an already active WiMAX session. If such match is detected, the AAA SHOULD deny network entry for the new network access attempt if the already existing session has an authenticated MAC address based on a successful device authentication, but the new entry has not.

The MS trying the new network entry, if not device-authenticated, should be considered a misbehaving device in case there is an already existing WiMAX session with an authenticated MAC address. If for the new network entry

the MS indicates an emergency network entry, this should be taken into account. However, the actual policy for how to deal with emergency network entry in this situation is up to the CSN operator's policy and depends on the local regulatory environment.

If as part of network access authentication a successful device authentication has been performed, the HAAA SHOULD include the MS-Authenticated attribute or AVP set to the value (1) in the Access-Accept message or WDEA command to indicate the successful device authentication and the resulting authenticated MAC address to the NAS.

The HAAA SHALL delete any keys once they are not needed. Specifically, the HAAA SHALL delete the MSK key after sending it Access-Accept packet to the NAS.

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 Accounting for additional prepaid procedures.

If Hot-Lining is active, that is if the user sessions is to be Hot-Lined then refer to section 4.4.3.5 for additional hot-lining procedures.

To support dynamic HA allocation in the home network, the HAAA SHALL include hHA-IP-MIP4, hHA-RK-KEY, hHA-RK-SPI and hHA-RK-Lifetime attributes in the RADIUS Access-Accept packet or the Diameter WDEA command at the end of successful Access Authentication. The generation of HA-RK, SPI and its lifetime is specified in section 4.3.5.1. The HAAA SHALL also include hHA-IP-MIP6 attribute in the RADIUS Access-Accept packet or Diameter WDEA command if MIP6 service is authorized for the MS.

The HAAA MAY alternatively authorize the dynamic HA allocation in the visited network, if the vHA-IP-MIP4 and vHA-IP-MIP6 attributes are included by the VAAA in the RADIUS Access-Request packet or the Diameter WDER command. In such case the HAAA SHALL echo the vHA-IP-MIP4 and vHA-IP-MIP6 attributes in the RADIUS Access-Accept or the Diameter WDEA command, and SHALL NOT include the hHA-IP-MIP4, hHA-IP-MIP6, hHA-RK-KEY, hHA-RK-SPI, and hHA-RK-Lifetime attributes.

The HAAA MAY also authorize the dynamic HA allocation in the visited network, if the vHA-IP-MIP4 and vHA-IP-MIP6 attributes are included by the VAAA in the RADIUS Access-Request packet or the Diameter WDER command, in addition to dynamic HA allocation in the home network. In this case, the HAAA SHALL include hHA-IP-MIP4, hHA-RK-KEY, hHA-RK-SPI and hHA-RK-Lifetime attributes, in addition to echoing the vHA-IP-MIP4 and vHA-IP-MIP6 attributes, in the RADIUS Access-Accept packet or the Diameter WDEA command at the end of successful Access Authentication. To support dynamic HA allocation, dynamic DHCP server allocation SHALL be supported for the DHCP Relay mode. The HAAA SHALL include the hDHCPv4-server address, hDHCP-RK, hDHCP-RK-Key-ID and hDHCP-RK-Lifetime attributes in the RADIUS Access-Accept packet or the Diameter WDEA command at the end of successful Access Authentication. The generation of DHCP-RK, ID and its lifetime is specified in section 4.3.6.1. The HAAA SHALL also include the hDHCPv6-server attribute in the RADIUS Access-Accept packet or the Diameter WDEA command if IPv6 service is authorized for the MS. The HAAA SHALL echo the IP address attribute of the vDHCPv4-server or the IP address attribute of the vDHCPv6-server in the RADIUS Access-Accept packet or the Diameter WDEA command, if these were originally included by VAAA in the Access-Request and the HAAA authorizes the assignment.

If the MS is attaching to a NAP to which the HNRP is directly connected, the HAAA server MAY include one or more Framed-IPv6-Prefix attributes in the final RADIUS Access-Accept packet or Diameter WDEA command.

If Mobility access Classifier of the MS is fixed or nomadic and the serving BS identification information received in the RADIUS Access-Request or Diameter WDER command does not belong to the MS network entry zone, the HAAA server SHALL deny network entry. In this case the HAAA may initiate a network rejection procedure as per section 4.5.1.2 to inform the MS about applying mobility restrictions. When initiating a network rejection procedure the HAAA SHALL set the rejection code 0x0C01 (Access outside defined Service Area). If the HAAA does not initiate a network rejection procedure, it SHALL generate and send a RADIUS Access-Reject or Diameter WDEA with Result-Code AVP indicating failure to the NAS (except when Hot-Lining is to be used per section 4.4.3.5.3).

If the Mobility Access Classifier of the MS is fixed or nomadic, H-AAA server SHALL include the Mobility Access Classifier in the RADIUS Access-Accept or Diameter WDEA command. The H-AAA server MAY initiate an EAP notification exchange as per section 4.12.7 to notify the MS about applying mobility restrictions and pass data related to the MS network entry zone.



#### 4.4.1.4.4.1 HAAA Processing

##### 4.4.1.4.4.1.1 Initial Request

The HAAA receives a RADIUS Access-Request packet containing a username attribute or Diameter WDER command with EAP-Payload AVP set to the NAI value received in an EAP-Response Identity from the MS.

The HAAA plays the role of the EAP authentication server and based on the locally provisioned information, suggests an EAP method by sending an Access-Challenge packet as defined in [52] containing an EAP message attribute with the suggested EAP method in the case of RADIUS. In the case of DIAMETER the HAAA responds with and WDEA commands with Result-Code AVP set to “DIAMETER\_MULTI\_ROUND\_AUTH” and the EAP-Payload AVP contain the suggested EAP method.

The HAAA caches the value sent in the username attribute and the NAS-Identifiers (NAS-ID, NAS-IP, NAS-IPv6).

If the MS rejects the EAP method proposed then it will send an EAP-NAK EAP method, carried in the next Access-Request packet or WDER command proposing another EAP method. If the HAAA accepts the new method or has an alternate method it will respond with a RADIUS Access-Challenge message as specified in [52] or Diameter WDEA with Result-Code AVP indicating multi-round authentication. This continues until an EAP method is selected, or until there are no more options in which case the HAAA SHALL respond with a RADIUS Access-Reject or Diameter WDEA with Result-Code AVP indicating failure.

Once the EAP method is agreed upon, the EAP method is executed by exchanges of RADIUS Access-Request/Access-Challenge packets or Diameter WDER/WDEA commands.

Once the EAP method completes execution, the HAAA SHALL respond with a final RADIUS Access-Accept packet or a final Access-Reject packet or Diameter WDEA packet with Result-Code AVP indicating success or failure.

The generation of the final Access-Accept or WDEA is specified in section 4.4.1.4.4.1.2.

##### 4.4.1.4.4.1.2 Final Response

Upon successful network access authentication the HAAA SHALL send a RADIUS Access-Accept packet as defined in Table 5-5 or Diameter WDEA command as specified in Table 5-22.

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

Upon successful network access authentication the HAAA SHOULD initiate MS network exit for any existing WiMAX session with a MS using the same MAC address as indicated in the Calling-Station-ID information if the existing WiMAX session is using a different Authenticator (if the authenticator is the same for both sessions, the authenticator will trigger network exit instead).

The HAAA SHOULD reject any new network entry for a MS that is using the same MAC address as an already existing WiMAX session in the case where the existing WiMAX session has an authenticated MAC address based on a successful device authentication but the new session has not.

The MS trying the new network entry, if not device-authenticated, should be considered a misbehaving device in case there is an already existing WiMAX session with an authenticated MAC address. If for the new network entry the MS indicates an emergency network entry, this should be taken into account. However, the actual policy for how to deal with emergency network entry in this situation is up to the CSN operator's policy and depends on the local regulatory environment.

Upon unsuccessful authentication the HAAA SHALL send a RADIUS Access-Reject packet as defined in Table 5-5 and specified in [52] or Diameter WDEA command with Result-Code AVP set to indicate failure.

##### 4.4.1.4.4.1.3 Processing Session Termination Request

As per RFC3588 [54] a Diameter capable NAS is required to send a Diameter WiMAX Session Termination Request (WSTR) command to the HAAA when a session terminates. Upon receiving such a command, a Diameter based HAAA SHALL respond back to the NAS with a WiMAX Session Termination Answer (WSTA) command as defined by RFC3588 [54].

The AVPs to be included in the WSTR/WSTA are listed in section 5.5.

#### 4.4.1.5 Reauthentication

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

Re-authentication procedures MUST NOT change the negotiated R3/R5 WiMAX version for that WiMAX Session.

##### 4.4.1.5.1 Reauthentication Triggers

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

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

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

- “AK Grace Time” is reached (the pre-configured time before PMK/ AK lifetime expiry);
- “CMAC\_PN\_\* counter Grace Interval” is reached (CMAC\_PN\_U or CMAC\_PN\_D counter reaches some pre-configured number before its maximum value, e.g., value bigger than  $2^{32} - 10,000$ );
- “CMAC\_KEY\_COUNT Grace Interval” is reached (CMAC\_KEY\_COUNT counter reaches some pre-configured number before its maximum value).

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

- “PMK Grace Time” is reached (the pre-configured time elapses before PMK lifetime expires);
- “CMAC\_KEY\_COUNT Grace Interval” is reached (CMAC\_KEY\_COUNT counter reaches some pre-configured number before its maximum value).

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

- Authenticator receives a message from the Serving BS (*AR\_EAP\_Start* message with BS-originated trigger TLV) informing it that MS' security context in the BS is going to expire (AK Context in a BS - CMAC\_PN\_\* counters, etc.);
- Authenticator receives *AR\_EAP\_Start* message from the Serving BS (in the case the MS instigates reauthentication by sending protected PKMv2 EAP-Start message).

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

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

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

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

- When it receives *AR\_EAP\_Start* message from the Serving BS (e.g., MS instigates reauthentication by sending protected PKMv2 EAP-Start message and the Serving BS forwards *AR\_EAP\_Start* to the “new” Authenticator in the Serving ASN).
- Upon its own decision .

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

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

#### 4.4.1.5.2 Reauthentication Process

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

##### 4.4.1.5.2.1 Reauthentication Initiation Phase:

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

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

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

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

##### 4.4.1.5.2.2 EAP Phase

EAP phase starts when an Authenticator sends EAP-Request/ Identity message over *AR\_EAP\_Transfer*. EAP phase ends after the successful EAP method completion when security material (MSK) is created in a supplicant and an authentication server, MSK key is delivered to an Authenticator in ASN and PKMv2 EAP-Transfer message with EAP-Success payload is sent to the MS.

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

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

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

##### 4.4.1.5.2.3 PKMv2 3-way Handshake (3WHS) Phase

PKMv2 3-way Handshake (3WHS) process SHALL be performed after EAP phase completion to enforce the “next” PMK context. The Authenticator triggers PKMv2 3WHS start in the Serving BS by sending *Key\_Change\_Directive* message including the “next” security context. After the Serving BS detects the successful completion of the PKMv2 3WHS and ensures that the MS uses the new security context over the air, the BS sends *Key\_Change\_Cnf* message to the Authenticator including Key Change Indicator TLV, thus indicating the completion of PKMv2 3WHS and the enforcement of the “next” security context.

At this moment, the Serving BS deletes the “old” MS’ security context and, in the case of Authenticator relocation, the Serving BS stops handling the “old” Authenticator ID and marks the “new” Authenticator as the active one.

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

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

#### 4.4.1.5.2.4 Reauthentication Completion Phase

This final stage of Reauthentication process is triggered by indication about reauthentication attempt completion (either successful or unsuccessful). When no Authenticator relocation occurs, such a trigger may be *Key\_Change\_Cnf* message with Key Change Indicator TLV indicating the results of PKMv2 3way handshake between BS and MS. In the case Authenticator relocation is in progress, the “new” Authenticator SHALL indicate its results to the “old” Authenticator using *Relocation\_Complete\_Req* message with Authentication Result TLV.

When “old” Authenticator receives a signal that reauthentication attempt failed to complete, i.e. due to failed transport and not because of receiving the RADIUS Access-Reject with EAP Failure indication, it SHOULD terminate “reauthentication lock” state, thus allowing new reauthentication attempts. “Old” Authenticator MAY also instigate new reauthentication attempt by itself.

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

If there was no Authenticator relocation, the Authenticator receiving *Key\_Change\_Cnf* message with Key Change Indicator TLV indicating “success” should terminate “reauthentication lock” state and SHALL delete the old MS security context (MSK/ PMK, AKs, CMAC\_KEY\_COUNT, etc.) assuming the successful completion of Reauthentication process.

In the scenario with Authenticator relocation, the “new” Authenticator, detecting the successful reauthentication completion, SHALL communicate this event with the “old” Authenticator (using *Relocation\_Complete\_Req* message with Authentication Result TLV set to indicate “success”). The “old” Authenticator receiving this indication SHALL stop acting as the Authenticator function for this MS.

The “new” Authenticator MAY also request some more MS context (e.g., MS Authorization Context, etc.) from the “old” Authenticator using Context Purpose Indicator TLV included in *Relocation\_Complete\_Req* message.

If there was no Context Purpose Indicator TLV requesting MS context in *Relocation\_Cnf* message, the “old” Authenticator SHALL respond with *Relocation\_Complete\_Rsp* message without any additional information and delete the MS’ context. Otherwise, if *Relocation\_Complete\_Req* contains Context Purpose Indicator TLV indicating the request for some MS context, the “old” Authenticator SHALL provide the requested context in *Relocation\_Complete\_Rsp* message and wait for the acknowledgement, *Relocation\_Complete\_Ack*, from the “new” Authenticator (confirming that it has received the requested MS context). When receiving this acknowledgement (ACK message), the “old” Authenticator SHALL delete the MS’ context.

In the case when the “new” Authenticator and the MS’ Anchor GW are not collocated, the “new” Authenticator SHALL also update the MS’ Anchor GW (Anchor DP function) that Authenticator relocation has occurred (using *Context\_Rpt* message including the new Authenticator ID). This process may occur in parallel with update of the “old” Authenticator.

#### 4.4.1.5.3 Management of PMK SN During Reauthentication

In an MS, the PMK usage in re-authentication will always follow the rules defined in the section 4.3.2.

At the network side, if re-authentication occurs on the Anchor Authenticator, since the Anchor Authenticator knows PMK SN from the previous successful authentication, the PMK SN usage in re-authentication can simply follow the rules defined in the section 4.3.3. But when re-authentication occurs on a new Authenticator (different to Anchor Authenticator), and if there is no record for PMK SN used in the last authentication in the new Authenticator, the new Authenticator SHALL contact the “old” Anchor Authenticator to get the latest PMK SN which is transferred from the “old” Anchor Authenticator to the “new” Anchor Authenticator.

1 Authenticator SHALL know whether an authentication procedure is initial authentication or not, - when an initial  
2 authentication occurs on an Authenticator, it SHALL initialize the PMK SN from Zero, but for re-authentication, it  
3 SHALL use PMK SN from the last successful authentication (copied from the “old” Anchor Authenticator).

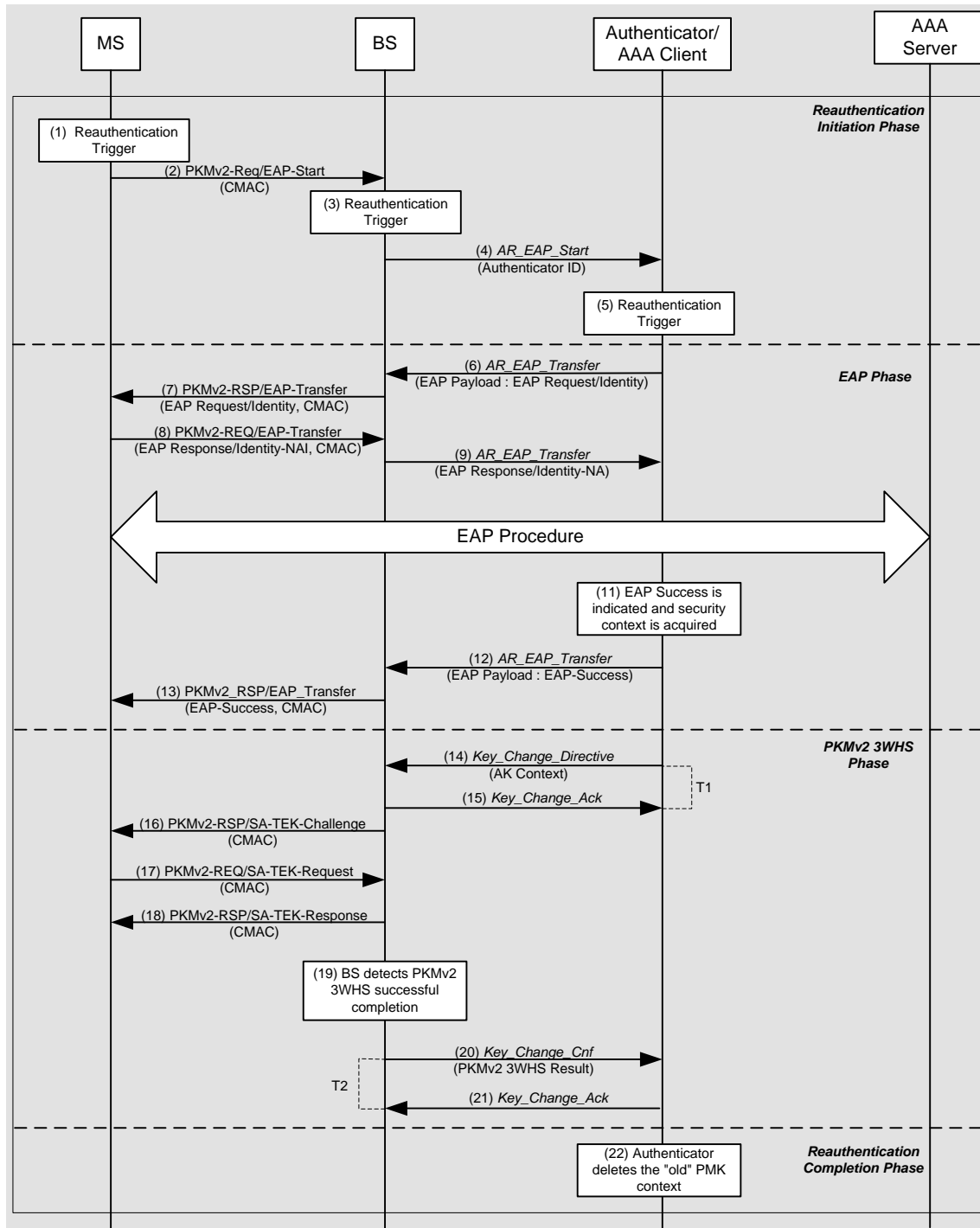
4 At the network side, current serving ASN can judge whether it is re-authentication or not as described in section  
5 4.4.1.5.5.

6 When EAP reauthentication process is successfully completed, (when the new Authenticator receives MSK from  
7 AAA server) the new Authenticator SHALL use the latest PMK SN. Then, in the “new” Authenticator, AK SN can  
8 be derived from PMK SN.

#### 9 **4.4.1.5.4 Reauthentication Process Without Authenticator Relocation**

10 EAP-based Reauthentication always starts from Authenticator/ ASN GW by sending EAP-Request/ Identity  
11 message over *AR\_EAP\_Transfer* to Serving BS. MS instigates the start of Reauthentication in the Network by using  
12 PKMv2 EAP-Start message protected with CMAC digest (using the currently active AK). Except for “EAP-Start”  
13 steps, MS-initiated and Network-initiated Reauthentication procedures (without involving Authenticator relocation)  
14 are the same. The Serving BS MAY instigate the start of Reauthentication (e.g., if it detects that MS security context  
15 in BS is going to expire), by issuing *AR\_EAP\_Start* message to the Authenticator.

16 The MS Reauthentication process not involving Authenticator relocation is shown in Figure 4-13:



**Figure 4-13 – Reauthentication Procedure (w/o Authenticator Relocation)**

### STEP 1

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

## STEP 2

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

## STEP 3

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

## STEP 4

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

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

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

If at the time of the BS sending the *AR\_EAP\_Start* message no value is assigned by the BS yet for this R6 context of the MS (e.g. due a recent handover of the MS to this BS), the BS SHALL assign a value for this R6 context of the MS and SHALL populate *R6\_Context\_ID* with this value. Assignment of the value is internal to the BS. However, the value SHALL uniquely identify this context of the MS at this BS. The BS SHALL add *R6\_Context\_ID* with the same value to all subsequent *AR\_EAP\_Transfer* and *Key\_Change\_Directive/Ack/Cng* messages belonging to the same authenticated MS and R6 context at this BS.

Serving BS handles the location of the current MS’ Anchor Authenticator. In the case the Serving BS and the MS’ Anchor Authenticator are located in the same ASN, the BS MAY choose to send *AR\_EAP\_Start* message directly to the current MS’ Anchor Authenticator (the “old” Authenticator). Otherwise, the BS sends *AR\_EAP\_Start* to its “default” Authenticator (the “new” Authenticator), thus triggering Authenticator relocation. The logic of how a BS decides whether to send *AR\_EAP\_Start* message to the “old” Authenticator or to its “default” Authenticator (when the Serving BS and the “old” Authenticator are both located in the same ASN), is implementation-specific.

The discussed scenario assumes no Authenticator relocation - Serving BS sends *AR\_EAP\_Start* to the current MS’ Anchor Authenticator (or the current MS’ Anchor Authenticator is collocated with BS’ “default” Authenticator).

The composition of *AR\_EAP\_Start* message is presented in Table 4-8:

**Table 4-8 – AR\_EAP\_Start**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier
MS Info	5.3.2.103	O	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.

IE	Reference	M/O	Notes
>BS-originated EAP-Start Flag	5.3.2.27	O	This flag is included when BS originates <i>AR_EAP_Start</i> 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).
BS Info	5.3.2.26	CM	Contains relevant Serving BS context in the nested IEs.
> BS ID	5.3.2.25	O	Serving BS ID.

This step is relevant only for MS-instigated Reauthentication.

## STEP 5

Reauthentication trigger occurs in the Authenticator.

## STEP 6

The Authenticator initiates EAP-based reauthentication (EAP Phase) by sending *AR\_EAP\_Transfer* message with EAP-Request/ Identity payload to the Serving BS. The composition of this message is presented in Table 4-9:

**Table 4-9 – AR\_EAP\_Transfer from Authenticator to BS (EAP Initiation)**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier
EAP Payload	5.3.2.62	M	EAP message. In this step it SHALL include EAP Identity Request message.

Note that *AR\_EAP\_Transfer* message composition remains the same through the EAP authentication process with only difference in the content of the EAP Payload TLV (containing different EAP messages).

If the authenticator received *AR\_EAP\_Start* prior to sending *AR\_EAP\_Transfer* and *AR\_EAP\_Start* from the BS included an *R6\_Context\_ID* TLV, the Authenticator SHALL include *R6\_Context\_ID* with the same value.

If the authenticator did not receive an *AR\_EAP\_Start* message (re-authentication triggered by the authenticator or AAA server) prior to sending *AR\_EAP\_Transfer* and does not have an assigned *R6\_Context\_ID* value for this R6 context, it SHALL include *R6\_Context\_ID* with the value set to “0”. Otherwise it SHALL include *R6\_Context\_ID* with the value set to the already assigned value.

If the authenticator receives *AR\_EAP\_Start* without an *R6\_Context\_ID* TLV included, the authenticator SHALL assume that this BS does not support the TLV, and SHALL not add the *R6\_Context\_ID* TLV in further R6 messages for this MS to the BS.

## STEP 7

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

If the BS receives an *R6\_Context\_ID* TLV in *AR\_EAP\_Transfer* with the value set to zero, the BS SHALL assign a value for this R6 context of the MS and SHALL populate *R6\_Context\_ID* with this value for all subsequent *AR\_EAP\_Transfer/Start* and *Key\_Change\_Directive/\_Ack/\_Cng* messages belonging to the same R6 context at this BS. Calculation of the value is internal to the BS.



1 If the BS receives an AR\_EAP\_Transfer message without an R6\_Context\_ID value from the authenticator, the BS  
2 SHALL assume that the authenticator does not support R6\_Context\_ID and SHALL not include R6\_Context\_ID in  
3 subsequent R6 messages for this R6 context.

#### 4 **STEP 8**

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

#### 8 **STEP 9**

9 After the successful CMAC digest verification, Serving BS forwards EAP payload (EAP-Response/ Identity) of the  
10 received PKMv2 EAP-Transfer message to the Authenticator using AR\_EAP\_Transfer message.

#### 11 **STEP 10**

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

16 In order to deliver the EAP payload to the AAA server, the Authenticator forwards the EAP message via a  
17 collocated AAA client using RADIUS Access-Request packets or Diameter WDER command containing the EAP  
18 payload.

19 The EAP authentication process (tunneling EAP authentication method) is performed between the MS and the  
20 Authentication server via the Authenticator in ASN GW in the same way as in the Initial Authentication. BS  
21 provides “relay” of EAP payload from PKMv2 EAP-related messages to AuthRelay and vice versa. The  
22 Authenticator in ASN GW acts in pass through mode (as described in [52]) and forwards the EAP messages  
23 received as a payload from the BS in AuthRelay messages to the AAA server using RADIUS Access-Request  
24 packets or Diameter WDER commands and vice versa – transferring EAP payload from RADIUS Access-Challenge  
25 packets or WDEA commands to AuthRelay. The composition of RADIUS packets is presented in section 5.4.1 and  
26 Diameter commands in section 5.5.1.1. Service-Type attribute (type 6, [37]) is set to the value “Authenticate only”  
27 during reauthentication.

28 During reauthentication, the NAS requests “Authentication only” from the AAA, and the AAA doesn't send any  
29 authorization profiles to the NAS.

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

#### 33 **STEP 11**

34 The Authenticator receives indication about the successful completion of EAP-based authentication and the required  
35 security context (i.e., MSK key and its lifetime). The indication about successful completion of EAP process is  
36 delivered using RADIUS Access-Accept packet from AAA server with EAP-Success message encapsulated in  
37 “EAP message” attribute or using Diameter WDEA command with EAP- Success message encapsulated in the  
38 EAP-Payload AVP and Result-Code AVP indicating successful authentication.

39 From this moment, Authenticator SHALL hold two security contexts: the currently active one and the “next” context  
40 created during re-authentication (Authenticator SHALL NOT override the currently active MSK key and its  
41 lifetime). Authenticator continues to provide AK key (e.g., for re-entry) using the currently active security context  
42 and uses the “next” security context only to derive AK Context for Key\_Change\_Directive (refer to the step 14).

43 If Authenticator receives the RADIUS Access-Reject with EAP Failure indication or Diameter WDEA command  
44 with EAP-Failure encapsulated in the EAP-Payload AVP and Result-Code AVP indicating authentication failure,  
45 the Authenticator SHALL trigger the MS Network Exit as described in Table 4-23. Note, that an incomplete

Reauthentication process such as due to failed transport SHALL NOT result in service termination for the MS as long as the “currently active” MSK and security context are valid.

#### STEP 12

The Authenticator forwards EAP results (EAP-Success or EAP-Failure message) to BS as EAP Payload TLV in *AR\_EAP\_Transfer* message.

#### STEP 13

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

#### STEP 14

The Authenticator sends *Key\_Change\_Directive* message to the BS to provide it with the “next” security context (AK Context) and trigger PKMv2 3WHS process between the BS and the MS (to enforce the “next” security context). The composition of this message is presented in Table 4-10:

**Table 4-10 – Key\_Change\_Directive from Authenticator to BS**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.
BS Info	5.3.2.26	M	Contains BS-related context in the nested IEs.
>AK Context	5.3.2.6	O	This compound parameter includes AK context parameters (AK, AK SN, AK lifetime, etc.) for BS use. This compound TLV is mandatory if authentication is successful.
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>BSID	5.3.2.25	M	
Authentication Complete	5.3.2.17	M	Contains authentication result and PKM2 message code.
>Authentication Result	5.3.2.18	M	
>PKM2 Message Code	5.3.2.134	M	
Certified-MS-Feature-List-for-BS	5.3.2.183	O <sup>1</sup>	Contains Allowed certified MS feature List for BS

Note <sup>1</sup>: This TLV SHALL be present if Certified-MS-Feature-List-for-BS is received as part of RADIUS/DIAMETER message.

If Authenticator receives the RADIUS Access-Reject or Diameter WDEA with EAP Failure indication, the Authenticator SHALL trigger MS Network exit as described in table 4-21.

#### STEP 15

BS receiving *Key\_Change\_Directive* message from Authenticator will acknowledge it by sending the *Key\_Change\_Ack* message.

#### STEP 16 - 18

The BS initiates PKMv2 3-way handshake (SA-TEK-Challenge/Request/Response exchange) with the MS to verify the new AK. The “next” security context (the “new” AK context) SHALL be used to protect PKMv2 3way handshake messages as specified in [11].

#### STEP 19

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

#### STEP 20

The BS indicates the completion of PKMv2 3WHS and enforcement of the “new” keys to the Authenticator by sending *Key\_Change\_Cnf* message with Key Change Indicator TLV.

**Table 4-11 – Key\_Change\_Cnf Message from BS to Authenticator (PKMv2 3WHS Completion)**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.
Failure Indication	5.3.2.69	O	
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”.
BS Info	5.3.2.26	M	
>BSID	5.3.2.25	M	

In the case, the BS detects a failure of PKMv2 3WHS process for any reason, it sends *Key\_Change\_Cnf* message with Key Change Indicator TLV Result set to indicate “failure”.

#### STEP 21

The Authenticator receiving *Key\_Change\_Cnf* message from the BS, acknowledges it by sending the *Key\_Change\_Ack* message.

**Table 4-12 – Key\_Change\_Ack**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.
Failure Indication	5.3.2.69	O	

## STEP 22

The Authenticator recognizing that the “new” AK context has been successfully enforced over the air, SHALL delete the “old” security context and change the status of the “new” security context from “next” to “active”. New MN-FA and FA-HA security information is also sent if required to the Anchor DPF/FA in the Context\_Rpt message sent from the Authenticator to the Anchor DPF/FA. This security information may be used by the FA if the subsequent Mobile IP re-registration is performed if required.

### 4.4.1.5.5 Reauthentication with Authenticator Relocation or Authenticator and FA Relocation

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

- In the case MS instigates Reauthentication process by PKMv2 EAP-Start message and the BS sends *AR\_EAP\_Start* message to its “default” Authenticator entity, which is different from the “old” Authenticator (the current MS’ Anchor Authenticator).
- In the case the Serving ASN (different from the Authenticator ASN) triggers Reauthentication process.
- In the case Reauthentication process is instigated by the “old” Authenticator (the current MS’ Anchor Authenticator), the Serving ASN MAY trigger FA relocation if FA is collocated with the Authenticator. (If the FA is not collocated with the Authenticator, the FA relocation may be rejected. In this case to trigger FA relocation, it should follow the procedure defined in section 4.8.2.3 or section 4.8.2.4.

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

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

- Receiving *AR\_EAP\_Start* from a BS. This means that MS has sent a protected PKMv2 EAP-Start message (signed by CMAC), BS has successfully verified it according to the currently active AK context and “relayed” EAP-Start to the ASN GW (where the “new” Authenticator entity is located) using *AR\_EAP\_Start* message.
- In the case the Serving ASN triggers Reauthentication by itself, it is aware whether MS is authenticated and authorized.
- In the case the “old” Authenticator instigates Reauthentication process in the ASN GW (e.g., the Serving ASN GW), R4 message informs this ASN GW that it is Reauthentication.

The “new” Authenticator learns the location of the “old” Authenticator during Reauthentication initiation phase. For MS-instigated reauthentication, Authenticator ID is delivered to the “new” Authenticator in *AR\_EAP\_Start* message. For network-initiated Reauthentication, it is delivered in the explicit R4 signal for “push” mode (e.g., from the “old” Authenticator).

In the case of Authenticator relocation, until Reauthentication process is completed, the Serving BS handles the IDs of both Authenticators – the “old” Authenticator and the “new” one. Once the Reauthentication process is completed, the trigger for renewing Proxy MIP4 Session is generated if the mobility mode is set to PMIP4. Refer to section 4.8.2.3 for further details on Proxy MIP4 Session renewal procedure.

#### 4.4.1.5.5.1 R3/R5 Version alignment during Authenticator Relocation

Authentication Relocation SHALL NOT proceed if any of the cases listed below are true:

- The R3/R5 WiMAX version supported by the “old” Authenticator does not match the R3/R5 WiMAX version supported by the “new” Authenticator
- The R3/R5 capabilities negotiated by the “old” Authenticator are not supported by the “new” Authenticator.

The following subsections provide examples of special cases of Authenticator Relocation when at least one Authenticator involved in relocation does not support version negotiation (e.g. WiMAX Rel.1.0), while the other Authenticator supports version negotiation (e.g. Rel.1.5).

##### 4.4.1.5.5.1.1 New Authenticator (WiMAX-Release “1.0” ASN) PULLs from Old Authenticator (WiMAX-Release “1.5”, “1.0” ASN)

New authenticator sends *Relocation\_Notify* message as explained in section 4.4.1.5.5.2

Upon receiving the message, the “old” authenticator (WiMAX-Release “1.5”) knows:

- What versions and capability the New authenticator has (via R4/R6 capability negotiation) and
- What are the needs of the WiMAX-Session that is requested to be moved.

The old authenticator sends *Relocation\_Notify\_Rsp* message with either Success or Failure

- Success - if the version negotiated for the WiMAX Session is supported by the New ASN GW (WiMAX-Release “1.0”). The new Authenticator performs AAA authentication procedure and new authenticator sends authentication results to the old authenticator as explained in section 4.4.1.5.5.2.
- Failure - if the version negotiated for the WiMAX Session is NOT supported by the New ASN GW (WiMAX-Release “1.0”). The Authenticator relocation fails.

##### 4.4.1.5.5.1.2 New Authenticator (WiMAX-Release “1.5”, “1.0” ASN) PULLs from Old Authenticator (WiMAX-Release “1.0” ASN)

This is a normal authentication relocation PULL procedure as explained in section 4.4.1.5.5.2.

##### 4.4.1.5.5.1.3 Old Authenticator (WiMAX-Release “1.5”, “1.0” ASN) PUSH to New Authenticator (WiMAX-Release “1.0” ASN)

“Old” Authenticator will only initiate Authenticator Relocation PUSH (as explained in section 4.4.1.5.5.3) if the WiMAX-Release negotiated for that session was at “1.0”

##### 4.4.1.5.5.1.4 Old Authenticator (WiMAX-Release “1.0” ASN) PUSH to New Authenticator (WiMAX-Release “1.5”, “1.0” ASN)

This is a normal authentication relocation PUSH procedure as explained in section 4.4.1.5.5.3.

##### 4.4.1.5.5.1.5 Old Authenticator (WiMAX-Release “1.0” ASN) PUSH to New Authenticator (WiMAX-Release “1.5” ASN)

“New” Authenticator (WiMAX-Release “1.5” ASN) rejects the PUSH procedure.

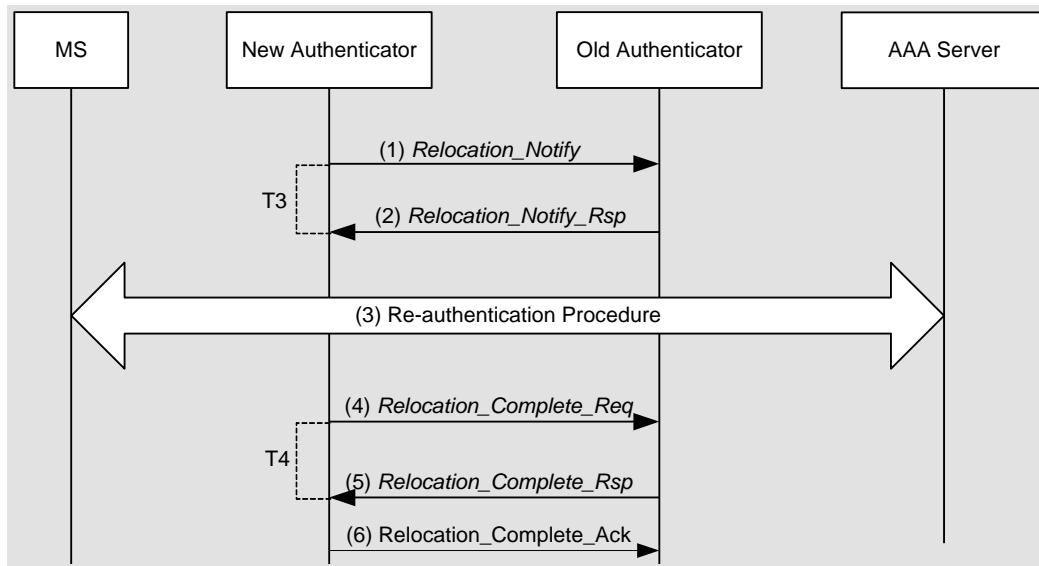
#### 4.4.1.5.5.2 Authenticator Relocation - “PULL” Mode

Authenticator relocation “pull” mode is considered when:

- MS or the Serving BS instigate Reauthentication process and the Serving BS sends *AR\_EAP\_Start* to the “new” Authenticator entity in the Serving ASN, or
- Serving ASN triggers Reauthentication process and may trigger FA relocation process.

Figure 4-14 presents Authenticator relocation “pull” mode.

- 1 If reauthentication is triggered by MS or BS, BS forwards *AR\_EAP\_Start* to the “new” Authenticator. In this case,
- 2 BS SHALL include Old authenticator ID with *AR\_EAP\_Start* message.
- 3 Triggering of FA relocation is outlined in 4.4.1.5.5.



**Figure 4-14 – 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 4-13:

**Table 4-13 – Relocation\_Notify from “New” Authenticator to “Old” Authenticator**

IE	Reference	M/O	Notes
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 SN, Anchor MM Context may also be requested).
MS Info	5.3.2.103	O	Contains MS-related context in the nested IEs.
>Authenticator ID	5.3.2.19	O	Indicates the ID of the “new” Authenticator.

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 Anchor MM 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.

- 1 The “old” Authenticator responds to the “new” Authenticator with *Relocation\_Rsp* message including the requested
- 2 MS context. If FA is collocated with the “old” Authenticator, then “old” Authenticator may add the Anchor MM
- 3 Context in the response if requested by the serving ASN/ASN GW (“new” Authenticator).

4 **Table 4-14 – Relocation\_Notify\_Rsp from “Old” Authenticator to “New” Authenticator**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
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.
>Mobility Access Classifier	5.3.2.423	O	Indicates the mobility access classification of the subscriber. It Shall be included if the MS mobility access classifier is known at the Anchor Authenticator to be Fixed or Nomadic.
>Reattachment Zone	5.3.2.424	O	Indicates the mobility access classification of the subscriber. It Shall be included if the MS mobility access classifier is known at the Anchor Authenticator to be Fixed or Nomadic.
> MS Security History	5.3.2.108	M	MS Security history – PMK SN.
>>PMK SN	5.3.2.133	M	
>>MS NAI	5.3.2.105	M	
>>PMIP-Authenticated-Network-Identity	5.3.2.41	O	Include when assigned by AAA in the RADIUS Access-Accept or the Diameter WDEA. Indicate authorized PMIP NAI for use by PMIP Client.  The above enables the PMIP NAI context to be passed along with the MS NAI TLV during authenticator relocation.
>>Authorization Policy Support	5.3.2.21	M	
>>VAAA IP Address	5.3.2.201	O	If the MS is re-authenticating via the visited CSN, either VAAA IP Address or VAAA Realm or both SHALL be included.
>> VAAA Realm	5.3.2.202	O	If the MS is re-authenticating via the visited CSN, either VAAA IP Address or VAAA Realm or both SHALL be included.
> MS Authorization Context	5.3.2.100	M	Contains Authorization context parameters of the specific MS.
>>MS NAI	5.3.2.105	M	

IE	Reference	M/O	Notes
>>PMIP-Authenticated-Network-Identity	5.3.2.41	O	Include when assigned by AAA in the RADIUS Access-Accept or Diameter WDEA. Indicate authorized PMIP NAI for use by PMIP Client.  The above enables the PMIP NAI context to be passed along with the MS NAI TLV during authenticator relocation.
>>R3 WiMAX Capability	5.3.2.207	M	
>>> R3 WiMAX-Release	5.3.2.441	M	WiMAX release negotiated during Initial Network Entry.
>>>R3 Accounting Capabilities	5.3.2.208	M	This TLV SHALL be included if R3 WiMAX-Capability is included in the transmitted message.
>>R3 CUI	5.3.2.210	O	
>>R3 Class	5.3.2.211	O	
>>R3 Framed IP Address	5.3.2.212	O	
>>R3 Framed-IPv6-Prefixs	5.3.2.213	O	
>>R3 Visited-Framed-IP-Address	5.3.2.362	O	
>>R3 Visited-Framed-IPv6-Prefixs	5.3.2.363	O	
>>R3 Framed-Interface-Ids	5.3.2.364	O	
>>R3 Visited-Framed-Interface-Ids	5.3.2.365	O	
>>R3 WiMAX Session ID	5.3.2.214	M	
>>R3 Packet Flow Descriptor	5.3.2.215	M	
>>>R3 Packet Data Flow ID	5.3.2.216	M	
>>>R3 Service Profile ID	5.3.2.218	O	This TLV May be included during Authenticator Relocation.
>>>R3 Uplink QoS ID	5.3.2.222	O	This TLV May be included during Authenticator Relocation.
>>>R3 Downlink QoS ID	5.3.2.223	O	This TLV May be included during Authenticator Relocation.
>>>SFID	5.3.2.184	M	Associated SFID (one or two).
> REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.



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

IE	Reference	M/O	Notes
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
> State	5.3.2.355	O	State attribute as received in most recent message from AAA server.
> Anchor MM Context	5.3.2.11	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).
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.
>>MIP4 Info	5.3.2.96	M	Mobility context of the MS.
>>>HA IP Address	5.3.2.75	M	IP address of the current HA.
>>>Home Address (HoA)	5.3.2.77	M	Home Address (HoA).
>>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA).
>>>Registration Lifetime	5.3.2.147	M	The remaining Mobile IP registration lifetime (measured in seconds).
Context Purpose Indicator	5.3.2.36	M	Bitmap indicating the required context.

Old authenticator MAY reject *Relocation\_Notify* only in the case that it is in “re-authentication lock” state.

### STEP 3

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

When reauthentication happens, the new authenticator SHOULD compare the realm and routing part of Outer-Identity which was used in the old authenticator. If the realm and routing part of the NAI is different, the new Authenticator SHALL discard the EAP-Response message from the MS.

### STEP 4

The “new” Authenticator informs the “old” Authenticator about the completion of EAP reauthentication process by sending *Relocation\_Complete\_Req* message with Authentication Result TLV. This message may optionally include the request for MS Context, required context for accounting.

The composition of *Relocation\_Complete\_Req* message is presented in Table 4-15:

**Table 4-15 – Relocation\_Complete\_Req Message from “New” Authenticator to “Old” Authenticator**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	O	Indicates the requested context. This TLV may be included only if Authentication Result indicates “success”.
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”.
>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”.

### STEP 5

The “old” Authenticator, receiving *Relocation\_Complete\_Req* message with Authentication Result indicating “success”, terminates “reauthentication lock” state and deletes MS security keys.

The “old” Authenticator responds with *Relocation\_Complete\_Rsp* message. If *Relocation\_Complete\_Req* message has contained the request for some MS context, the “old” Authenticator responds with *Relocation\_Complete\_Rsp* message containing the requested MS context, Accounting context and waits for *Relocation\_Complete\_Ack* message (Optional Step6) from the “new” Authenticator. Otherwise, if *Relocation\_Complete\_Req* didn’t request any information, the “old” Authenticator may proceed with MS context deletion.

The composition of *Relocation\_Complete\_Rsp* message is presented in Table 4-16:

**Table 4-16 – Relocation\_Complete\_Rsp Message**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
PMIP4 Context	5.3.2.373	M	
>MIP4 Info	5.3.2.96	M	Mobility context of the MS.
>>HA IP Address	5.3.2.75	O	IP address of the current HA.
>>Home Address (HoA)	5.3.2.77	M	Home Address (HoA).
>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA).
>>Registration Lifetime	5.3.2.147	M	The remaining Mobile IP registration lifetime (measured in seconds).
MS Info	5.3.2.103	O	Contains MS-related context in the nested IEs.
>MS Authorization Context	5.3.2.100	O	Contains Authorization context parameters of the specific MS.
>>MS NAI	5.3.2.105	CM	This TLV SHALL be included if MS Authorization Context is included in the

IE	Reference	M/O	Notes
			transmitted message.
>>PMIP-Authenticated-Network-Identity	5.3.2.41	O	Include when assigned by AAA in the RADIUS Access-Accept or Diameter WDEA. Indicate authorized PMIP NAI for use by PMIP Client. The above enables the PMIP NAI context to be passed along with the MS NAI TLV during authenticator relocation.
>>R3 WiMAX Capability	5.3.2.207	CM	This TLV SHALL be included if MS Authorization Context is included in the transmitted message.
>>> R3 WiMAX-Release	5.3.2.441	CM	WiMAX release negotiated during Initial Network Entry. This TLV MAY be included if R3 WiMAX-Capability is included in the transmitted message.
>>>R3 Idle Notification Capabilities	5.3.2.209	O	This TLV MAY be included if R3 WiMAX-Capability is included in the transmitted message.
>>R3 CUI	5.3.2.210	O	
>>R3 Class	5.3.2.211	O	
>>>R3 Accounting Capabilities	5.3.2.208	CM	This TLV SHALL be included if R3 WiMAX-Capability is included in the transmitted message.
>>R3 Framed IP Address	5.3.2.212	O	
>>R3 Framed-IPv6-Prefixs	5.3.2.213	O	
>>R3 Visited-Framed-IP-Address	5.3.2.362	O	
>>R3 Visited-Framed-IPv6-Prefixs	5.3.2.363	O	
>>R3 Framed-Interface-Ids	5.3.2.364	O	
>>R3 Visited-Framed-Interface-Ids	5.3.2.365	O	
>>R3 WiMAX Session ID	5.3.2.214	CM	This TLV SHALL be included if MS Authorization Context is included in the transmitted message.
>>R3 Packet Flow Descriptor	5.3.2.215	CM	This TLV SHALL be included if MS Authorization Context is included in the transmitted message.
>>>R3 Packet Data Flow ID	5.3.2.216	CM	This TLV SHALL be included if R3 Packet Flow Descriptor is included in the transmitted message.
>>>R3 Service Profile ID	5.3.2.218	O	This TLV May be included during Authenticator Relocation.
>>>R3 Uplink QoS ID	5.3.2.222	O	This TLV May be included during Authenticator Relocation.
>>>R3 Downlink QoS ID	5.3.2.223	O	This TLV May be included during Authenticator

IE	Reference	M/O	Notes
			Relocation.
>>>>SFID	5.3.2.184	CM	Associated SFID (one or two). This TLV SHALL be included if R3 Packet Flow Descriptor is included in the transmitted message.
>REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per Frame Support	5.3.2.296	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
Accounting Context	5.3.2.204	O	Accounting Context.
>Accounting Mode Provisioning	5.3.2.243	CM	This TLV SHALL be included if Accounting Context is included in the transmitted message.
>>Accounting Type	5.3.2.247	CM	This TLV SHALL be included if Accounting Mode Provisioning is included in the transmitted message.
>> Interim Update Interval	5.3.2.248	O	The Interim Update Interval is a data field in the AAA server and sent to the Accounting Client in the RADIUS Access-Accept packet or the Diameter WDEA command. This TLV is only used for volume-based accounting and thus managed by Accounting Agent. It may be provided in Accounting context if the Anchor Accounting Client is collocated with Anchor Accounting Agent.
>>Accounting Number of ToDs	5.3.2.256	O	The number of Time of Day Tariff Switch TLVs.
>>Time of Day Tariff Switch	5.3.2.253	O	The Time of Day Tariff Switch TLV is a data field in the AAA server and sent to the ASN-GW in the RADIUS Access-Accept packet or the Diameter WDEA command. There can be more than one of these sent.
>>>Time of Day Tariff Switch Time	5.3.2.254	CM	The time of day time in hours and minutes. This TLV SHALL be included if Time of Day Tariff Switch is included in the transmitted

IE	Reference	M/O	Notes
			message.
>>>Time of Day Tariff Switch Offset	5.3.2.255	CM	The time of day timezone offset This TLV SHALL be included if Time of Day Tariff Switch is included in the transmitted message.
>R3 Acct Session Time	5.3.2.361	O	The number of seconds the flow or session was active.
>R3 Active Time	5.3.2.286	O	The number of seconds the session was not in Idle Mode.
Context Purpose Indicator	5.3.2.36	O	Bitmap indicating the required context.
PPAC	5.3.2.65	O	Describes the Prepaid Capabilities of the ASN.
>AvailableInClient	5.3.2.89	CM	This TLV SHALL be included if PPAC is included in the transmitted message.

## STEP 6

**Table 4-17 – Relocation\_Complete\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

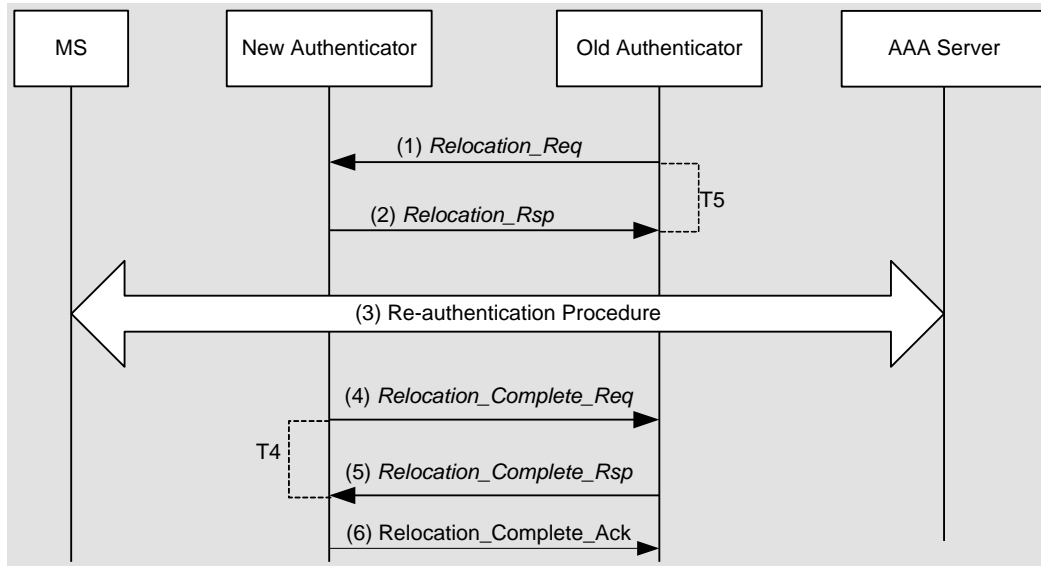
If Relocation\_Complete\_Rsp message from the “old” Authenticator contained any MS context, the “new” Authenticator acknowledges it with Relocation\_Complete\_Ack message (no TLVs). Otherwise, this step is not required.

The “old” Authenticator receiving Relocation\_Complete\_Ack message may proceed with MS context deletion.

### 4.4.1.5.5.3 Authenticator Relocation -- “PUSH” mode

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

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



**Figure 4-15 – Authenticator Relocation (PUSH)**

### STEP 1

The “old” Authenticator sends *Relocation\_Req* message to a New Authenticator in order to request reauthentication attempt start. The “old” Authenticator also enters “reauthentication lock” state preventing any new reauthentication attempt start. The “old” Authenticator may include also some relevant MS context (e.g., PMK SN) in this message. The “Old” Authenticator may add Anchor MM Context in *Relocation\_Req* message if FA is collocated.

The composition of *Relocation\_Req* message is presented in Table 4-18:

**Table 4-18 – Relocation\_Req from “Old” Authenticator to “New” Authenticator**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>Mobility Access Classifier	5.3.2.423	O	Indicates the mobility access classification of the subscriber. It Shall be included if the MS mobility access classifier is known at the Anchor Authenticator to be Fixed or Nomadic.
>Reattachment Zone	5.3.2.424	O	Indicates the list of BS IDs allowed for reattachment. It Shall be included if the MS mobility access classifier is known at the Anchor Authenticator to be Fixed or Nomadic.
> MS Security History	5.3.2.108	M	Provides MS Security history – PMK SN.
>>PMK SN	5.3.2.133	M	
>>MS NAI	5.3.2.105	M	



IE	Reference	M/O	Notes
>>PMIP-Authenticated-Network-Identity	5.3.2.41	O	Include when assigned by AAA in the RADIUS Access-Accept packet or the Diameter WDEA command. Indicate authorized PMIP NAI for use by PMIP Client.  The above enables the PMIP NAI context to be passed along with the MS NAI TLV during authenticator relocation.
>>Authorization Policy Support	5.3.2.21	M	
>>VAAA IP Address	5.3.2.201	O	If the MS is re-authenticating via the visited CSN, either VAAA IP Address or VAAA Realm or both SHALL be included.
>> VAAA Realm	5.3.2.202	O	If the MS is re-authenticating via the visited CSN, either VAAA IP Address or VAAA Realm or both SHALL be included.
> MS Authorization Context	5.3.2.100	M	Contains Authorization context parameters of the specific MS.
>>MS NAI	5.3.2.105	M	
>>PMIP-Authenticated-Network-Identity	5.3.2.41	O	Include when assigned by AAA in the RADIUS Access-Accept or Diameter WDEA. Indicate authorized PMIP NAI for use by PMIP Client.  The above enables the PMIP NAI context to be passed along with the MS NAI TLV during authenticator relocation.
>>R3 WiMAX Capability	5.3.2.207	M	
>>>R3 Accounting Capabilities	5.3.2.208	M	
>>> R3 WiMAX-Release	5.3.2.441	M	WiMAX release negotiated during Initial Network Entry.
>>R3 CUI	5.3.2.210	O	
>>R3 Class	5.3.2.211	O	
>>R3 Framed IP Address	5.3.2.212	O	
>>R3 Framed-IPv6-Prefixs	5.3.2.213	O	
>>R3 Visited-Framed-IP-Address	5.3.2.362	O	
>>R3 Visited-Framed-IPv6-Prefixs	5.3.2.363	O	
>>R3 Framed-Interface-Ids	5.3.2.364	O	
>>R3 Visited-Framed-Interface-Ids	5.3.2.365	O	
>>R3 WiMAX Session ID	5.3.2.214	M	
>>R3 Packet Flow Descriptor	5.3.2.215	M	

IE	Reference	M/O	Notes
>>>R3 Packet Data Flow ID	5.3.2.216	M	
>>>R3 Service Profile ID	5.3.2.218	O	This TLV May be included during Authenticator Relocation.
>>>R3 Uplink QoS ID	5.3.2.222	O	This TLV May be included during Authenticator Relocation.
>>>R3 Downlink QoS ID	5.3.2.223	O	This TLV May be included during Authenticator Relocation.
>>>SFID	5.3.2.184	M	Associated SFID (one or two).
> REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per Frame Support	5.3.2.296	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
> Authenticator ID	5.3.2.19	O	Indicates the ID of the ‘old’ Authenticator GW.
> State	5.3.2.355	O	State attribute as received in most recent message from AAA server.
> Anchor MM Context	5.3.2.11	O	Contains FA Context for the MS, If included it indicates the suggestion for FA relocation.
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.
>>MIP4 Info	5.3.2.96	M	Mobility context of the MS.
>>>HA IP Address	5.3.2.75	M	IP address of the current HA.
>>>Home Address (HoA)	5.3.2.77	M	Home Address (HoA).
>>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA).
>>>Registration Lifetime	5.3.2.147	M	The remaining Mobile IP registration lifetime (measured in seconds).
BS Info	5.3.2.26	O	Contains relevant Serving BS context in the nested IEs.

IE	Reference	M/O	Notes
> BS ID	5.3.2.25	CM	Serving BS ID.

## STEP 2

The “new” Authenticator entity responds to the “old” Authenticator with *Relocation\_Rsp* message.

**Table 4-19 – Relocation\_Rsp from “New” Authenticator to “Old” Authenticator**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Accept/ Reject Indicator	5.3.2.1	M	Indicates Accept/ Reject of the corresponding request.

## STEP 3

In the case, the Serving ASN responds with *Relocation\_Rsp* message indicating a “reject” of Authenticator relocation “push”, the Anchor Authenticator MAY initiate MS Network Exit procedure- 6.

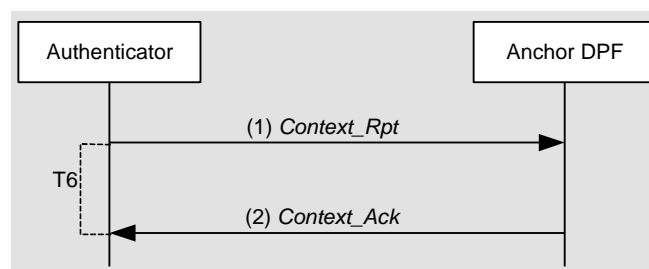
The procedure is same as that of Authenticator Relocation procedure (PULL).

### 4.4.1.5.5.4 Authenticator Relocation PUSH and PULL modes collision

In case of Authenticator Relocation PUSH and PULL modes collision, Old Authenticator SHALL follow pull procedure initiated by New Authenticator. New Authenticator SHALL ignore incoming *Relocation\_Req* and Old Authenticator SHALL abort its *Relocation\_Req* transaction.

### 4.4.1.5.5.5 Authenticator Update Notification Procedure

After authenticator relocation procedure happens, new authenticator SHALL inform the Anchor DP of the change of authenticator by sending *Context\_Rpt* which includes the new authenticator ID. New MN-FA (in case of CMIP only) and FA-HA security information is also sent to the Anchor DPF/FA which is used if the subsequent Mobile IP re-registration is performed.



**Figure 4-16 – Authenticator Update Notification Procedure**

## STEP 1

The “new” Authenticator updates the MS’ Anchor DP with the “new” MS’ Anchor Authenticator location using *Context\_Rpt* message. The composition of this *Context\_Rpt* message is presented in Table 4-20:

**Table 4-20 – Context\_Rpt from “New” Authenticator to Anchor DP/FA**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Provide failure indication for this message.
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	5.3.2.181	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 Authorization Context” and may include “FA context” (bits #1, #3 and #4).
FA Security Info	5.3.2.372	O <sup>3</sup>	Contains updated security information. This information is needed for the subsequent Mobile IP re-registration after the re-authentication is performed.
MIP4 Security Info	5.3.2.266	O	
>MN-FA key	5.3.2.98	O	Push MN-FA key to FA.
>MN-FA SPI	5.3.2.99	O	SPI of MN-FA key.
>MN-FA Key Lifetime	5.3.2.267	O	Time of MN-FA key remaining valid.
>FA-HA Key	5.3.2.66	O	Push FA-HA key to FA. (in case of CMIP only)
>FA-HA Key SPI	5.3.2.68	O	SPI of FA-HA key. (in case of CMIP only)
>FA-HA Key Lifetime	5.3.2.67	O	Time of FA-HA key remaining valid. (in case of CMIP only)

## STEP 2

Anchor DP receiving *Context\_Rpt* message, acknowledges it by *Context\_Ack* message and overrides the Authenticator ID value.

**Table 4-21 – Context\_Ack from Anchor DP/FA to “New” Authenticator**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Provide failure indication for this message.

### 4.4.1.5.6 Error Handling During Reauthentication

If Authenticator receives the RADIUS Access-Reject packet with EAP Failure indication or Diameter WDEA command with Result-code AVP indicating an EAP Failure, the Authenticator SHALL trigger the MS Network Exit as described in table 4-21. Note, that an incomplete Reauthentication process such as due to failed transport SHALL NOT result in service termination for the MS as long as the “currently active” MSK and security context are valid.

<sup>3</sup> FA Security Information may be excluded if the security association between the MN-FA and FA-HA are not supported. Otherwise, this TLV must be present in the Context\_Rpt message sent from the Authenticator to the FA.

#### 4.4.1.5.6.1 Timers and Timing Considerations

This section defines the timer that the entities participating in the Re-authentication procedure SHALL use. The Re-authentication procedure uses six timers:

- T1: is started by the Authenticator when it sends a Key\_Change\_Directive message to BS and is stopped upon receiving the corresponding Key\_Change\_Ack.
- T2: is started by the BS when it sends a Key\_Change\_Cnf message to Authenticator and is stopped upon receiving the corresponding Key\_Change\_Ack.
- T3: is started by the New Authenticator when it sends Relocation\_Notify message to Old Authenticator and is stopped upon receiving the corresponding Relocation\_Notify\_Ack.
- T4: is started by the New Authenticator when it sends Relocation\_Complete\_Req message to Old Authenticator and is stopped upon receiving the corresponding Relocation\_Complete\_Rsp.
- T5: is started by the Old Authenticator when it sends Relocation\_Req message to New Authenticator and is stopped upon receiving the corresponding Relocation\_Rsp.
- T6: is started by the Authenticator when it sends Context\_Rpt message to Anchor DPF and is stopped upon receiving the corresponding Context\_Ack.
- T<sub>Relo\_Comp\_Rsp</sub>: is started by the Old Authenticator when it sends Relocation\_Complete\_Rsp message to the New Authenticator with the requested context and is stopped upon receiving the corresponding Relocation\_Complete\_Ack.

Table 4-22 defines the default timer values and also indicates the range of the recommended duration of these timers.

**Table 4-22 – Timers and Timing Considerations**

Timers	Default Values (msec)	Maximum Timer Value (msec)
T <sub>1</sub>	TBD	TBD
T <sub>2</sub>	TBD	TBD
T <sub>3</sub>	TBD	TBD
T <sub>4</sub>	TBD	TBD
T <sub>5</sub>	TBD	TBD
T <sub>6</sub>	TBD	TBD
T <sub>Relo_Comp_Rsp</sub>	TBD	TBD

#### 4.4.1.5.6.2 Error Handling Scenarios

Table 4-23 defines the lists the various error conditions during Re-authentication.

**Table 4-23 – Error Handling Scenarios**

Error Condition	Failure Case	Action
1	Authenticator receives the RADIUS Access-Reject or the	Authenticator SHALL initiate the MS Network exit.

Error Condition	Failure Case	Action
	Diameter WDEA with EAP Failure indication	
2	Incomplete Reauthentication process such as due to failed transport	MS current session SHALL NOT be terminated as long as the “currently active” MSK and security context are valid.
3	BS detects PKMv2 3-way hand shake failure	BS sends Key_Change_Cnf message with Key Change Indicator TLV set to indicate “failure”. MS current session SHALL NOT be terminated as long as the “currently active” MSK and security context are valid. Authenticator SHOULD initiate another Reauthentication.
4	Authenticator Relocation Fails	New/Old Authenticator sends Relocation_Rsp/Relocation_Notify_Rsp message with Accept/Reject Indicator TLV set to indicate error cause in the case of failure.

#### 4.4.1.5.6.3 Timer Expiry

Table 4-24 shows the details of the corresponding action(s) associated with timer expiry. Upon each timer expiry, if maximum retries has not exceeded, the related message is retransmitted and timer is restarted. Otherwise corresponding action(s) should be performed as indicated in Table 4-24.

**Table 4-24 – Actions after Timer Max Retry**

Timers	Entity where Timer Started	Action(s)
T1	Authenticator	May initiate MS Network Exit (as described in section 4.5.2.1.1).
T2	BS	May initiate MS Network Exit (as described in section 4.5.2.1.1).
T3	New Authenticator	May initiate MS Network Exit (as described in section 4.5.2.1.1).
T4	New Authenticator	May initiate MS Network Exit (as described in section 4.5.2.1.1).
T5	Old Authenticator	May initiate MS Network Exit (as described in section 4.5.2.1.1).
T6	Authenticator	May initiate MS Network Exit (as described in section 4.5.2.1.1).
T <sub>Relo_Comp_Rsp</sub>	Old Authenticator	May initiate MS Network Exit (as described in section 4.5.2.1.1).

#### 4.4.1.6 Network Service Capability Negotiation and Authorization

WiMAX network can provide Simple IP, CMIP (IPv4 or IPv6) or PMIP services (IPv4 or IPv6) as well as Simple Ethernet and MIP based Ethernet services in the case of Ethernet services support to the subscriber based on service provider business requirement, subscriber profile, network architecture and network entity capability information, etc. In order to successfully provide the user service several major network entities should be involved. These

network entities are, ASN, VCSN and HCSN. Each network entity may support multiple network service related functionalities. Whether the Simple IP service or PMIP or CMIP, or Simple Ethernet or MIP based Ethernet service is invoked by the network for a given user depends on network service capability negotiation result among ASN, VCSN and HCSN along with the home operator policy.

The Network Service Capability Negotiation Scheme and related functional requirement are defined in the following sections. The scheme expands the network access authentication and authorization process adding capability to negotiate the appropriate network service among ASN, VCSN (when exists) and HCSN. Two new AAA attributes named ASN Network Service Capability and VCSN Network Service Capabilities have been defined to indicate IP and optional ETH service capabilities of ASN and VCSN, respectively. Capabilities that may be associated with the ASN include DHCPv4 Relay, DHCPv6 Relay, DHCPv4 Proxy, DHCPv6 Proxy, L2 DHCP Relay, FA, PMIP Client, AR with IPv4 transport, AR with IPv6 transport, MAG (including the additional PMIP6 Security Info attribute), L2FW, Ethernet Service FA etc. The commonly expected VCSN Network Capabilities are v-DHCPv4 Server, v-DHCPv6 Server, MIP-HAv4, MIP-HAv6, PMIP6 LMA, Ethernet Service HA, eCB and potentially other functionalities.

These two parameters should be conveyed from ASN, VCSN (if exists) to H-CSN through RADIUS Access-Request packet or Diameter WDER command. The HAAA in HCSN SHALL make the final decision on type of network service(s) that is authorized for particular subscriber, based on the capability information received from corresponding ASN and VCSN network entities, subscriber profile, and its own home network policy. The HAAA in HCSN SHALL pass Authorized Network Services attribute (and Visited Authorized Network Service, if VCSN service anchoring is permitted) along with the necessary network configuration information (such as HA IP address, DHCP Server IP address etc.) to the ASN through VCSN by using RADIUS Access-Accept packet or Diameter WDEA command. Once the NAS in ASN obtains the Authorized Network Services attribute and network configuration information, it SHALL store this information locally and make it available to use by the appropriate Network service related function entities. Depending on the outcome of the network service authorization scheme, the ASN will accordingly provide Simple IP, PMIP or CMIP, or in the case of Ethernet services, Simple Ethernet or MIP based Ethernet, with the HCSN or VCSN anchoring, to the MS at the point when MS attempts to obtain the network service. It is the network that will make the final decision of whether or not to allow to the MS the network service request, and will assign the appropriate network service support for this MS.

#### **4.4.1.6.1 NAS Requirement for Network Service Capability Negotiation**

The NAS SHALL include the ASN Network Service Capability attribute within the WiMAX-Capability VSA of the RADIUS Access-Request packet or Diameter WDER command and forward them towards HAAA in HCSN through AAA-Proxy in VCSN (if VCSN exist).

When the R3 reference point is only IPv4-based, the NAS in the ASN supporting PMIP6 SHALL include the IPv4 transport indication flag in the PMIP6-Service-Info attribute of the RADIUS Access-Request or Diameter WDER command.

If NAS receives Authorized Network Services attribute within WiMAX-Capability VSA of the RADIUS Access-Accept packet or Diameter WDEA command, the NAS SHALL store this information locally and use this as the indication of which network services with the HCSN-anchoring have been authorized for the MS. If the NAS received the Visited Authorized Network Services attribute within WiMAX-Capability VSA, the NAS MAY decide to assign a network service anchored in the VCSN according to the policy decision.

HAAA in HCSN SHALL send a RADIUS Access-Reject or Diameter WDEA command indicating authentication failure to the NAS if it cannot authorize any of the network services that NAS supports. If the NAS receives a RADIUS Access-Accept, or Diameter WDEA indicating successful authentication which requires ASN to provide a network service that it cannot support, then it SHALL treat the successful authentication as a rejected authentication Access-Accept/Access-Reject.

If NAS receives Simple IPv4 authorization through the Authorized Network Services attribute (or Visited Authorized Network Services attribute) in the RADIUS Access-Accept or Diameter WDEA command WiMAX-Capability VSA, the NAS SHALL store this information locally and make it available to be used later for Simple IPv4 service.

If NAS receives Simple IPv6 authorization through the Authorized Network Services attribute (or Visited Authorized Network Services attribute) in the RADIUS Access-Accept or Diameter WDEA command WiMAX-



1 Capability VSA, the NAS SHALL store this information locally and make it available to be used later for Simple  
2 IPv6 service.

3 If NAS receives either vHA-IP-MIP4 or hHA-IP-MIP4 attributes in RADIUS Access-Accept packet or Diameter  
4 WDEA command, the NAS SHALL store these HAv4 attributes locally and make it available to be used later for  
5 either CMIP4 or PMIP4 services to the MS.

6 If NAS receives either vHA-IP-MIP6 and/or hHA-IP-MIP6 attributes in RADIUS Access-Accept packet or  
7 Diameter WDEA command, the NAS SHALL store these HAv6 attributes locally and make it available to be used  
8 later for CMIP6 services to the MS.

9 If NAS receives either vLMA-IPv6-PMIP6 and/or hLMA-IPv6-PMIP6 attributes in RADIUS Access-Accept  
10 message or Diameter WDEA command the NAS SHALL store these PMIP6 attributes locally and make available  
11 later for PMIP6 service, if assigned to the MS. The NAS SHALL also process and store PMIP6 protocol feature  
12 authorization hints provided in the PMIP6-Service-Info attribute. If NAS has indicated IPv4 R3 transport capability  
13 to the HAAA, the vLMA-IPv4-PMIP6 and/or hLMA-IPv4-PMIP6 attributes in RADIUS Access-Accept or  
14 Diameter WDEA SHALL be processed and stored.

15 If NAS receives Simple ETH Service authorization through the Authorized Network Service attribute (or Visited  
16 Authorized Network Services attribute) in the RADIUS Access-Accept or Diameter WDEA command WiMAX-  
17 Capability VSA, the NAS SHALL store this information locally and make it available to be used later for Simple  
18 Ethernet service.

19 If NAS receives MIP based ETH Service authorization through the Authorized Network Service attribute and  
20 Bootstrapping Mobility Service attribute of WiMAX-Capability VSA, i.e., either vHA-IP-MIP4 or hHA-IP-MIP4  
21 attributes, in RADIUS Access-Accept or Diameter WDEA command, the NAS SHALL store these attributes locally  
22 and make it available to be used later for MIP based Ethernet services to the MS.

23 If NAS receives either Simple ETH Service authorization or MIP based ETH Service authorization through the  
24 Authorized Network Service attribute in the WiMAX-Capability VSA in the RADIUS Access-Accept packet or  
25 Diameter WDEA command, the NAS SHALL discard the presence of the vDHCP Server or hDHCP Server  
26 attributes in the RADIUS Access-Accept or Diameter WDEA commands and SHALL provide the state of the L2  
27 DHCP Relay authorization locally, to indicate whether the L2 DHCP Relay functionality should be enabled for this  
28 MS.

29 If NAS receives either vDHCP or hDHCP Server attributes in RADIUS Access-Accept packet or Diameter WDEA  
30 command, the NAS SHALL store these attributes locally and make it available to be used in DHCP signaling  
31 transaction later. It also indicates that DHCP Relay functionality should be enabled for this MS.

32 If NAS does not receive DHCP Server attributes in RADIUS Access-Accept packet or Diameter WDEA command,  
33 it indicates that DHCP Proxy functionality should be enabled for this MS. The NAS SHALL store the IP and Host  
34 configuration attributes locally and make them available to be used in DHCP signaling transaction later. It also  
35 indicates that DHCP proxy functionality should be enabled for this MS.

#### 36 **4.4.1.6.2 VCSN Requirement for Network Service Capability Negotiation**

37 If VCSN AAA proxy receives the RADIUS Access-Request packet or Diameter WDER command from the NAS in  
38 ASN, the VCSN SHALL attach its own VCSN Network Service Capability attribute to the original RADIUS  
39 Access-Request packet or Diameter WDER command sent from ASN and forward this message to HAAA in HCSN.

40 VCSN SHALL attach vHA and/or vDHCP(v4 or v6) Server address to the RADIUS Access-Request packet or  
41 Diameter WDER message and forward to HAAA in HCSN if VCSN is capable of providing these services.

42 VCSN SHALL NOT provide a network Service that it is not authorized for in the RADIUS Access-Accept or  
43 Diameter WDEA command indicating successful authentication.

44 If the VCSN supports PMIP6 mobility management, the VAAA MAY append the LMA capability in the RADIUS  
45 Access-Request's VCSN Network Service Capability indication. In that case the IPv6 address of the LMA in the  
46 VCSN SHALL be present.

47 HAAA in HCSN SHALL send a RADIUS Access-Reject packet or Diameter WDEA command indicating failure to  
48 VCSN if it cannot authorize any of the network services that NAS supports. If the VCSN receives a RADIUS

Access-Accept or Diameter WDEA command, which requires it to support a network service that it cannot support, then it SHALL treat the RADIUS Access-Accept or Diameter WDEA command with successful authentication indication as an Access-Reject rejection.

#### 4.4.1.6.3 HCSN Requirement for Network Service Capability Negotiation

If HCSN receives the RADIUS Access-Request packet or Diameter WDER command the HCSN SHALL authorize the appropriate network service(s) for a given MS based on received ASN Network Service Capability, MS subscriber profile, home network policy information and (if exists) the VCSN Network Service Capability attributes. The HAAA in HCSN SHALL send RADIUS Access-Accept packet or Diameter WDEA command towards NAS in ASN, passing through VCSN in case MS is roaming. These RADIUS or Diameter messages Access-Accept packet SHALL include appropriate network service authorization and attributes associated with the corresponding network Service(s) as follows:

The HAAA SHALL include Authorized Network Services attribute to indicate the network service(s) anchored in the HCSN that the MS is authorized for.

The HAAA SHALL include Visited Authorized Network Services attribute to indicate for which network service(s), either IP or Ethernet, anchored in VCSN the MS is authorized for.

HAAA SHALL not authorize a network service that cannot be supported by both the CSN and ASN.

If HAAA has authorized CMIP4 or PMIP4 or MIP based ETH service, it SHALL include vHA-IP-MIP4 and/or hHA-IP-MIP4 attributes in the RADIUS Access-Accept packet or Diameter WDEA command.

If HAAA has authorized CMIP6 service, it SHALL include vHA-IP-MIP6 and/or hHA-IP-MIP6 attributes in the RADIUS Access-Accept packet or Diameter WDEA command.

If HAAA has authorized PMIP6 service, it SHALL include vLMA-IPv6-PMIP6 or hLMA-IPv6-PMIP6 attributes in the Access-Accept message or WDEA command. The HAAA SHALL also include PMIP6-Service-Info attribute indicating allowed PMIP6 protocol feature (v4 support, signaling protection mode). When IPv4 transport is available over R3 only, the HAAA SHALL include h/vLMA-IPv4-PMIP6 attribute(s). The HAAA MAY include address configuration parameters for PMIP6 if such information (home/visited HNP, home/visited IPv4 HoA) is available at the AAA server.

If HAAA includes VCSN or HCSN DHCP Server attributes, it indicates that HAAA has authorized use of DHCP Relay functionality in the ASN for IP Services. The HAAA SHOULD authorize DHCP Relay functionality only if the ASN previously indicated corresponding support.

If HAAA does not include VCSN or HCSN DHCP Server attributes for IP Services, it indicates authorized use of DHCP Proxy functionality in the ASN. The HAAA SHOULD authorize DHCP Proxy functionality only if the ASN previously indicated corresponding support

#### 4.4.2 EAP Authentication Relay

Authentication Relay protocol is a protocol among the suite of the WiMAX Protocols. Authentication Relay protocol is used as an envelope to transfer EAP payload (EAP messages) between BS (EAP Relay entity) and EAP Authenticator over R6 the UDP/ IP infrastructure, when the EAP Authenticator is collocated with the Serving ASN. AuthRelay protocol messages are defined to correspond to PKMv2 EAP-related messages in IEEE 802.16e. Authentication Relay protocol can be transferred over R6 or R4 by a stateless relay in the serving ASN when the EAP Authenticator is not collocated with the Serving ASN.

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

**Table 4-25 – List of Authentication Relay Protocol Messages**

<i>AR_EAP_Start</i>
<i>AR_EAP_Transfer</i>

The Base Station acts as an EAP Relay entity. It transfers an EAP message received from the MS over R1 to the Authenticator and vice versa. For each valid EAP message that the Base Station receives over PKMv2, it sends a

corresponding AuthRelay message to Authenticator (including the received EAP message as a payload). The BS processes only valid PKMv2 EAP-related MAC messages on the air interface and discards non-valid PKMv2 EAP-related messages (e.g., unprotected EAP-Start, unprotected EAP-Transfer during re-authentication, protected PKMv2 messages which BS fails to validate, etc.).

The AuthRelay messages represented by different Message Types correspond one-to-one to the PKMv2 EAP-related messages on 802.16e interface. The mapping between PKMv2 and AuthRelay messages is presented in Table 4-26.

**Table 4-26 – Authentication Relay Messages Mapping to PKMv2 and Vice Versa**

AuthRelay Message	PKMv2 message code	PKMv2 REQ/ RSP	Notes
<i>AR_EAP_Start</i>	EAP-Start	REQ	PKMv2 EAP-Start is sent by MS to initiate EAP reauthentication. <i>AR_EAP_Start</i> 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 <i>AR_EAP_Start</i> to the Authenticator PKMv2: MS → BS AuthRelay: BS → Authenticator
<i>AR_EAP_Transfer</i>	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

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

WiMAX Authenticator is collocated with AAA client and acts in a pass-through.

The Authenticator issues EAP messages over AuthRelay and transfers EAP messages as a payload between AuthRelay and AAA:

- Initiates EAP process by sending EAP identity request message over AuthRelay (using the appropriate AuthRelay Message Type);
- EAP message received on AuthRelay is transferred to the AAA server in EAP-Message attribute(s) of RADIUS Access-Request packet or Diameter WDER command;
- EAP message received in EAP-Message attribute(s) of RADIUS packets or Diameter commands is transferred to the BS over AuthRelay (using the appropriate AuthRelay Message Type).

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

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

### 4.4.3 Accounting

#### 4.4.3.1 Introduction

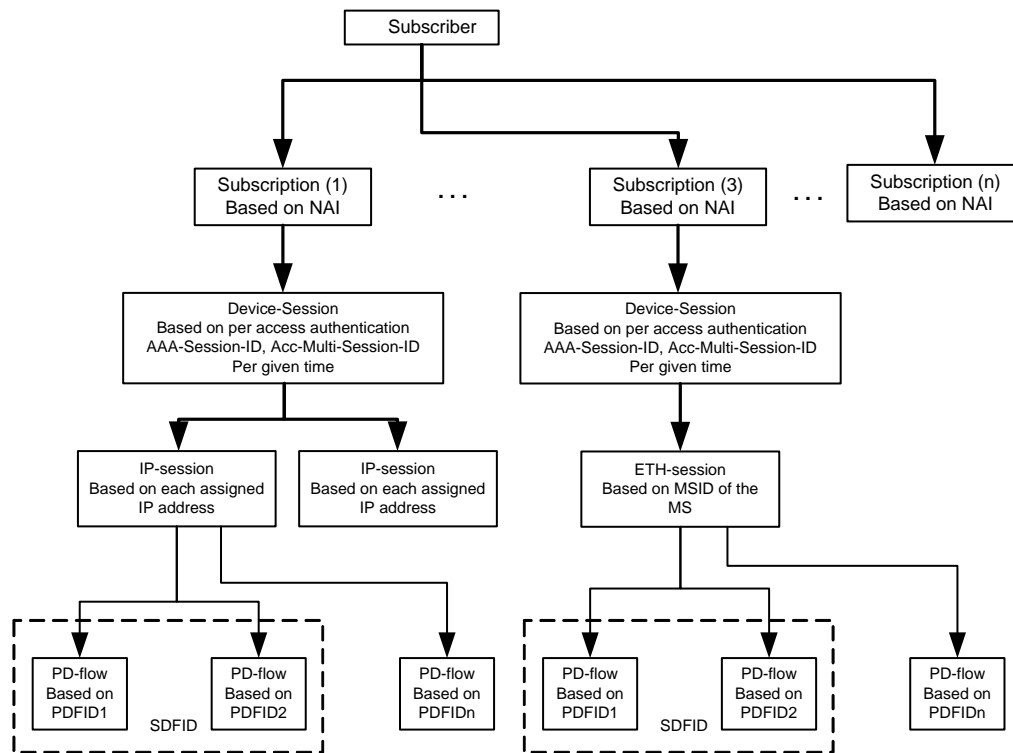
Both offline (post-paid) and online (prepaid) accounting, and hot-lining protocols and procedures are described in this section. The accounting will cover user billing while user is in home network or roaming.

#### 4.4.3.2 Accounting Modes and Terminology

This section details the terminology and supported accounting modes used in WiMAX.

Figure 4-17 shows the different possible levels and related identities or identifiers. Two different modes with different granularity for actual generation of accounting information are supported: IP-/ETH-session accounting and PD-flow accounting, or session-based accounting and flow-based accounting, as both modes apply for IP services as well as Ethernet services.

Depending on the CS choice session-based accounting is performed either depending of the IP-connectivity for IP-CS or depending of Layer-2 connectivity for ETH-CS.



**Figure 4-17 – Accounting Modes and Terminology**

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

**Table 4-27 – 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.

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

Accounting modes are defined in Table 4-28. Actual collection of accounting information happens either in IP-session mode for IP-CS, respectively in ETH-Session Mode for ETH-CS or in PD-flow mode, where ASN and CSN support for IP-session accounting and ETH-Session accounting if ETH-CS is supported is mandatory and support for PD-flow accounting is optional.

**Table 4-28 – Accounting Modes**

Accounting Mode	Description	ID
Session	<p>For IP Service:</p> <p>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.</p> <p>For Eth Service:</p> <p>One to one mapping between ETH-sessions and device-session. ETH-session is based on MSID of the MS.</p>	<p>For IP Service:</p> <p>IP address assigned to the MS.</p> <p>For ETH Service:</p> <p>MSID of the MS</p>
PD-flow	<p>If packet data flow-based accounting is used, there are one or more PD-flows mapping to the same IP-/ETH-session. A PD-flow can be mapped to one or more service flows (see QoS section for detailed mapping). Several PD-flows can be grouped by a service data flow, identified by an SDFID.</p>	PDFID, SDFID

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

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

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

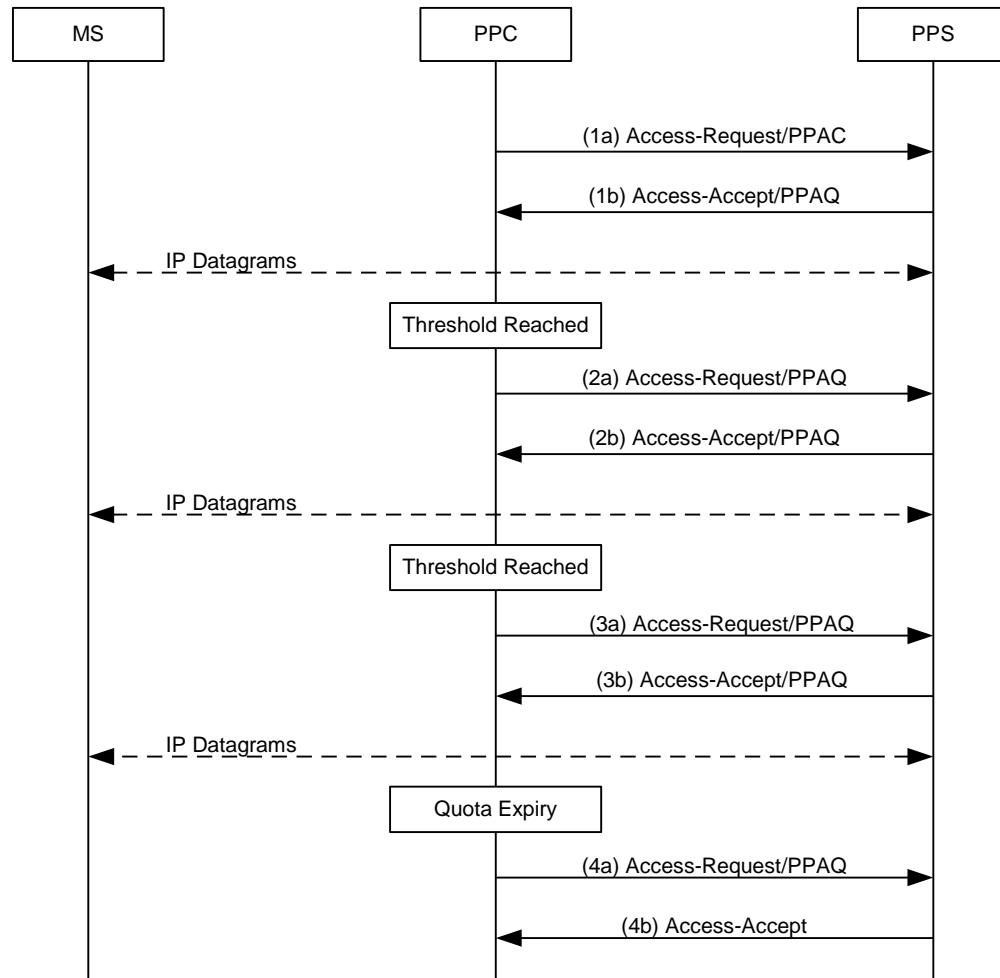
In RADIUS, the PPS is assumed to be collocated with the HAAA in the HCSN. The PPC is located at the ASN in the NAS and/or the HCSN or VCSN in the HA. In the event, HA is not present in the network, PPC may be located at the ASN. The PPC performs metering when it is in the bearer path. When the PPC is not on the bearer path, the PPA is responsible for metering the flows on behalf of the PPC and is located in the ASN at the bearer path (i.e., anchor DPF). The PPA communicates with the PPC over R4. The PPA is responsible for the quota management, and PPC acts as the proxy between PPA and PPS. The PPC maintains the parameters used to communicate with the PPS over R3 interface. These parameters should be transferred from old PPC to new PPC when authenticator relocation occurs. In RADIUS, quota information should be transferred from old PPA to new PPA when PPA relocation occurs. In Diameter, quota information transfer depends on the capability of the PPS. The PPA is collocated with the anchor DPF and will move with the anchor DPF during R3 relocation. The R3 relocation is described in the section 4.8.

[97] provides the specification for the operation of On-Line Accounting. This section describes the WiMAX specifics operation as they pertain to On-line accounting. Section 5.4.2 specifies the On-line RADIUS attributes.

##### 4.4.3.3.1 RADIUS based Procedures

On-line accounting is set up by the exchange of RADIUS Access-Request and Access-Accept packets. The initial Access-Request packet from the NAS and or the HA includes a prepaid accounting capability (PPAC) VSA to the

- 1 PPS indicating support for On-line accounting at the ASN and or the HA. If the Subscription Session requires on-
- 2 line charging the PPS assigns a prepaid accounting quota (PPAQ) to the PPC using RADIUS Access-Accept
- 3 packets. As the session continues, the PPC and the PPS replenish the quotas by exchanging RADIUS packets. A
- 4 typical on-line interaction is illustrated in Figure 4-18.
- 5 Off-line accounting SHALL also be used for subscribers that use Prepaid Services.



**Figure 4-18 – Online Accounting Procedures**

#### STEP 1a

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

#### STEP 1b

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

#### STEP 2a

Once the threshold for the quota(s) is reached, the PPC requests additional quota by sending an Authorize-Only 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 session-based (IP-session or ETH-session) or flow-based. For session-based quotas are allocated to each session. The Service-ID in the PPAQ SHALL be set to the IP-Address corresponding to the IP-Session as specified in section 5.4.2 for IP-CS and to the MSID for ETH-CS.

For flow-based accounting quotas are allocated to each packet data flow. The Service-ID attribute of the PPAQ SHALL identify the IP-/ETH-session and the flow. The format of this attribute is specified in section 5.4.2.

**4.4.3.3.2 Diameter based Procedures**

For Diameter based Online Charging R3-OC interface is defined between Anchor SFA and Online Charging System (OCS)/Pre-Paid Server (PPS). The definition of the basic functionalities and the protocol for R3-OC interface is based on IETF Diameter Credit Control Application (DCCA) [63]; in addition, Ro interface definition in [99] is also taken as an input, including its simplifications of, and enhancements to RFC4006 [63]. The basic mechanism of R3-OC is one in which the online charging/prepaid client requests resource allocation from, and reports credit control information to the online charging/prepaid server.

The corresponding message for the Debit/Reserve Unit Request operation in R3-OC is Credit-Control-Request (CCR) and for the Debit/Reserve Unit Response operation is Credit-Control-Answer (CCA), as specified in IETF RFC4006 [63].

To support the WiMAX specific requirements, including handling mobility, some WiMAX specific AVPs and re-Used AVPs with WiMAX specific parameters are defined on R3-OC interface. The design principle for R3-OC interface is to define a protocol as simple and as efficient as possible while satisfying WiMAX specific requirements.

The R3-OC interface is restricted to time-based and/or volume-based online charging on IP session, PD flows. Event based charging for WiMAX network is FFS.

Basically R3-OC interface is applicable to both PCC and non-PCC scenarios where in case of PCC it is called PCC-R3-OC as additional parameters might be present. In presence of PCC, charging rules from the PDF/PCRF are bound to specific SF flows, and charging information (e.g., AF-Charging-Information AVP) from Application Function (AF) may be attached in CCR message which might be used as charging correlator in the billing domain. For further details on PCC please see [3].

**4.4.3.3.2.1 R3-OC Interface Definition**

The R3-OC protocol is based on the Diameter Credit Control [RFC4006] protocol with additional optional AVPs.

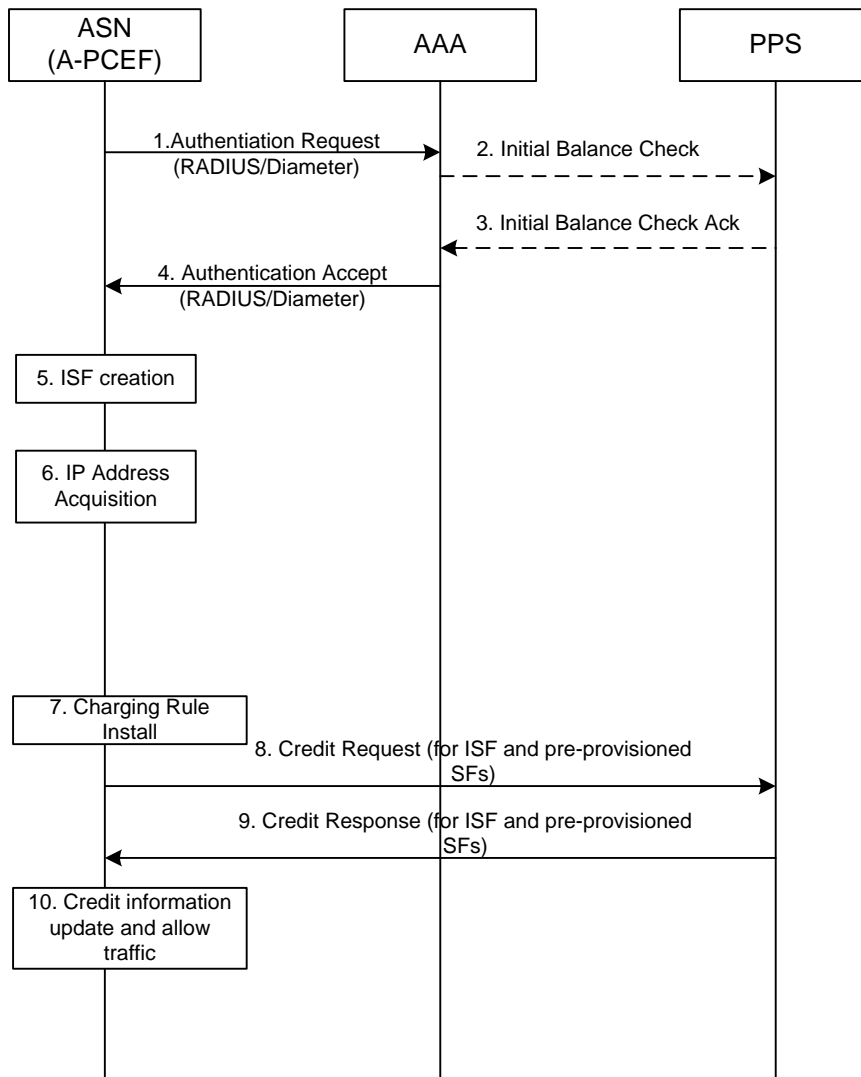
With regard to the Diameter protocol defined over the R3-OC interface, PPS acts as a Diameter online charging server, i.e., it is the network element that handles Credit Control Requests for a particular MS. The PPC acts as the

Diameter online charging client, i.e., it is the network element requesting credits from PPS, and returns the consumption information about the consumed credits to PPS.

For existing AVPs predefined vendor codes are used. For AVPs introduced by WiMAX, the WiMAX vendor ID SHALL be used.

#### 4.4.3.3.2.2 Session Establishment

Figure 4-19 depicts the message flows for initial and pre-provisioned service flow creation.



**Figure 4-19 – Initial and Pre-provisioned Service Flow Creation**

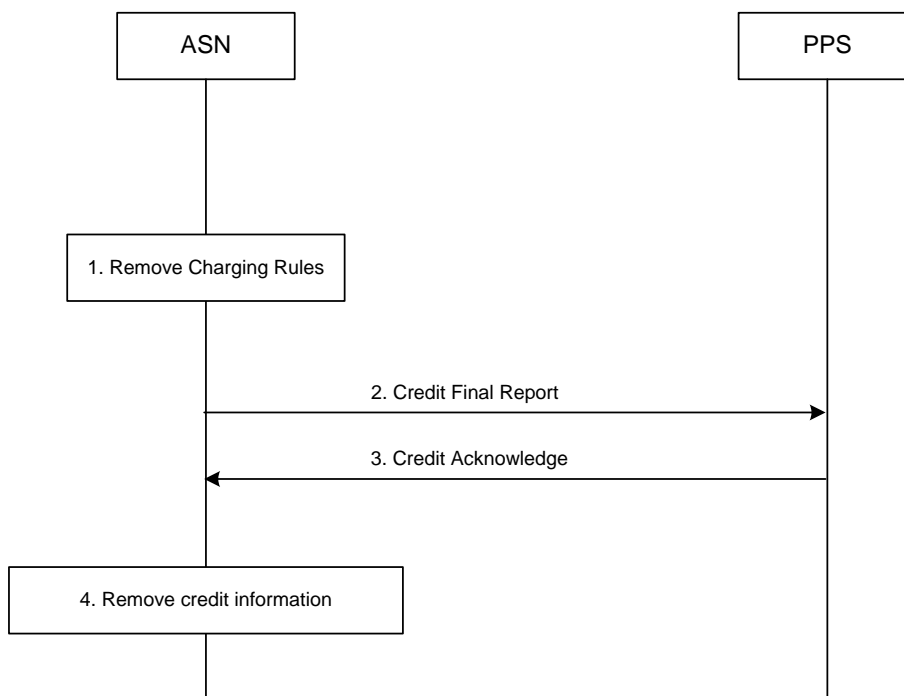
1. ASN initiates the Authentication request to the AAA server.
- 2-3. If the subscription profile requires online accounting, the AAA server checks the credit balance for this subscriber by exchanging information with the PPS (no quota information is provided; the information can be used by the AAA-server to estimate whether a quota request might be successful). Steps 2 and 3 are optional and specific to the operator's implementation. After this check the AAA-server may decide to reject the user authentication or trigger Hot-Lining.



- Note: the configuration of the AAA-server and the ASN GW / A-PCEF SHOULD be configured with the same PPS/OCS address.
4. The AAA server responds to the authentication request received in step 1 from the ASN and includes an indication that online accounting is required.
  5. ISF is created and resources are allocated to the MS. Optionally, pre-provisioned SFs could be created but traffic SHALL be blocked until PCRF authorizes traffic and PPS provides sufficient quota for the ISF/PPSF (see step 12).
  6. IP address is assigned but user traffic to CSN is blocked.
  7. Charging rules are installed.
  8. The ASN requests credit from the PPS for all pre-provisioned SFs and ISF.
  9. The PPS returns credit to the ASN for these SFs.
  10. The ASN updates credit information based on the information returned from PPS. ASN allows user traffic to be transferred to CSN. Furthermore, pre-provisioned SFs SHALL be created or modified (modification in case creation was already done in step 5). Blocking of the traffic SHALL be adjusted according to the information received from PCC and PPS.

#### 4.4.3.3.2.3 Session Termination

Figure 4-20 depicts the message flows for MS/SS/BS initiated session termination:



**Figure 4-20 –Session Termination**

1. ASN removes all policy and charging rules related with this IP-CAN session.
2. ASN issues final reports and returns the remaining credit to PPS.
3. PPS acknowledges the credit report.
4. ASN removes all credit information of this IP-CAN session.

#### 4.4.3.3.3 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 5.3.2.373. 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 (layer 3 and higher layer signaling transported in ISF) and user data packets and octet counts to/from the mobile. The Accounting Agent 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.

##### 4.4.3.3.3.1 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 [51] and therefore the NAS and HA do not need to include the STC attribute as specified in the appendix.

##### 4.4.3.3.3.2 HAAA Requirements

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

##### 4.4.3.3.4 Tariff Switching

Tariff switching with both the volume and duration based post-paid services are initiated at the Home AAA server.

##### 4.4.3.3.5 PPC Relocation in case of RADIUS based Online Accounting

Prepaid Client (PPC) is collocated with MS' Authenticator entity. During Authenticator relocation scenario described in the section [4.4.1.5.5], PPC is also relocated. Note, that quota is not handled in the PPC entity, so it is not impacted by PPC relocation. The specific Online Accounting Capabilities (described by AvailableInClient TLV) are enforced by PPA and not by PPC. So, online accounting capabilities of the "new" PPC do not have to be considered during PPC relocation.

The below figure describes the specifics relevant for PPC relocation.

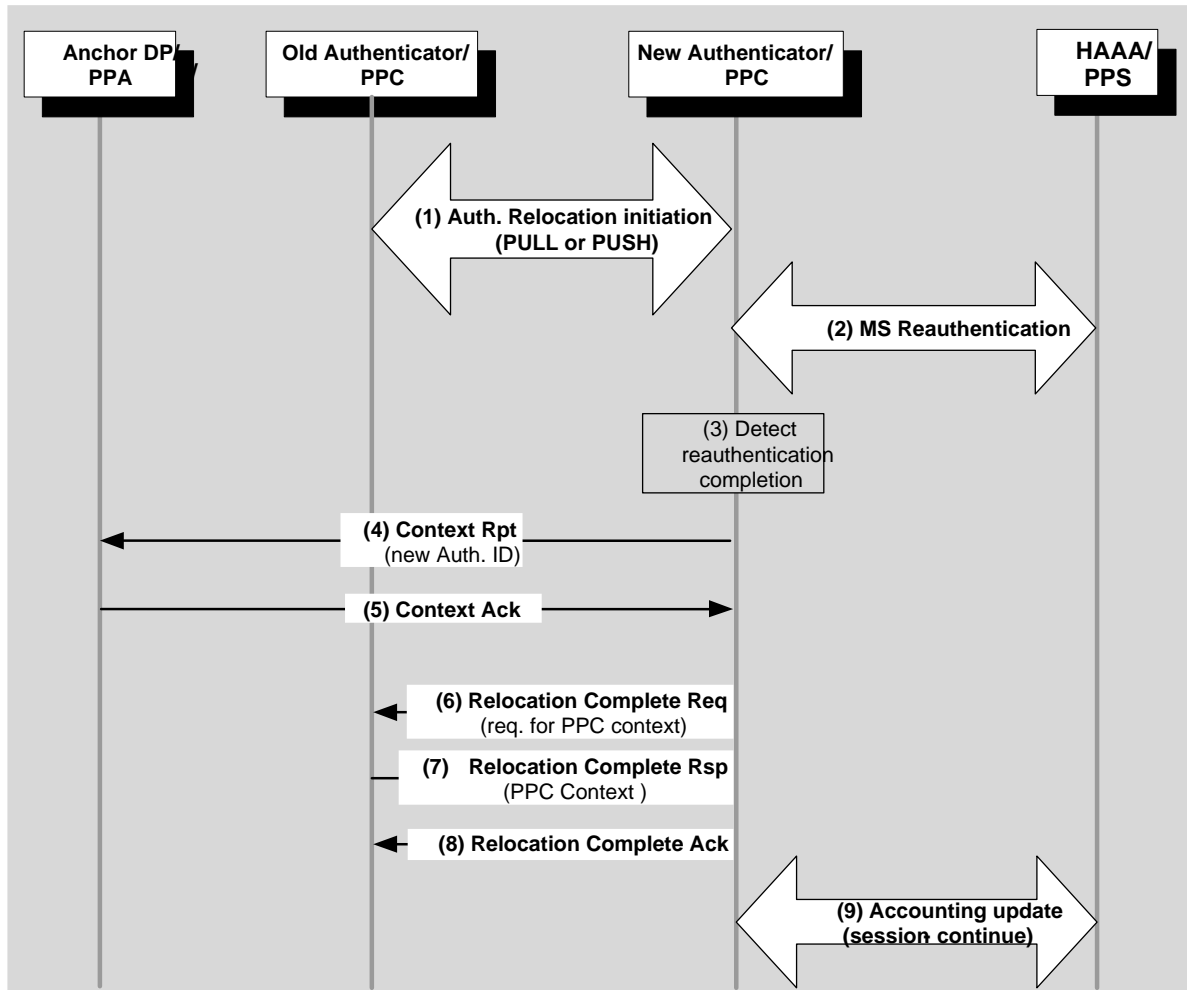


Figure 4-21 – PPC relocation

### STEP 1

Authenticator relocation is initiated (PUSH or PULL modes). In this step the “old” Authenticator indicates to the “new” authenticator that Online Accounting must be supported. The “old” Authenticator SHALL ensure that the “new” authenticator supports context transfer for Online Accounting. The negotiation of Online Accounting capabilities between the two ASN GWs/ Authenticators is done by setting Context Purpose Indicator bit indicating “Online Accounting Context” in R4 Authentication Relocation PUSH/ PULL messages (*Relocation\_Notify/Relocation\_Notify\_Rsp* and *Relocation\_Req* messages).

Specifically, in the PULL scenario, the “new” Authenticator should indicate its support of context transfer for online accounting by setting proper CPI in *Relocation\_Notify* message. The “old” Authenticator then may indicate the required online accounting mode in the *Relocation\_Notify\_Rsp* message using CPI bit. If the “old” Authenticator receives *Relocation\_Notify* message without CPI “online accounting context” bit set, then it SHALL assume that the “new” Authenticator does not support online accounting context transfer.

In the PUSH scenario, if context transfer for online accounting has been activated in the “old” Authenticator, it indicates this by setting the corresponding CPI bit in the *Relocation\_Req* message.

### STEP 2

MS Reauthentication occurs in the “new” Authenticator entity. This includes EAP Phase and PKMv2 3WHS Phase.

**STEP 3**

In the case the “new” Authenticator detects successful completion of reauthentication process (successful completion of PKMv2 3WHS Phase), it initiates R4 Relocation Complete transaction.

**STEP 4**

The “new” Authenticator/ PPC sends *Context\_Rpt* message to the Anchor DP/ PPA to update it with the new Authenticator location/ identity. From this moment, the PPA entity will communicate quota updates with the “new” PPC.

**STEP 5**

Anchor DP responds with *Context-Ack* message.

**STEP 6**

The “new” Authenticator informs the “old” Authenticator about the successful completion of reauthentication process by sending *Relocation\_Complete\_Req* message. The “new” Authenticator may set “Online Accounting context” bit in the Context Purpose Indicator TLV to indicate the request for PPC context.

**STEP 7**

The “old” Authenticator responds with *Relocation\_Complete\_Rsp* message providing MS context including PPC Context. The “new” Authenticator may create a new online charging session if a requested PPC context was not provided by the “old” Authenticator.

**STEP 8**

The “new” Authenticator confirms reception of *Relocation\_Complete\_Rsp* message by sending *Relocation\_Complete\_Ack*. When the “old” Authenticator receives this message it may delete MS context.

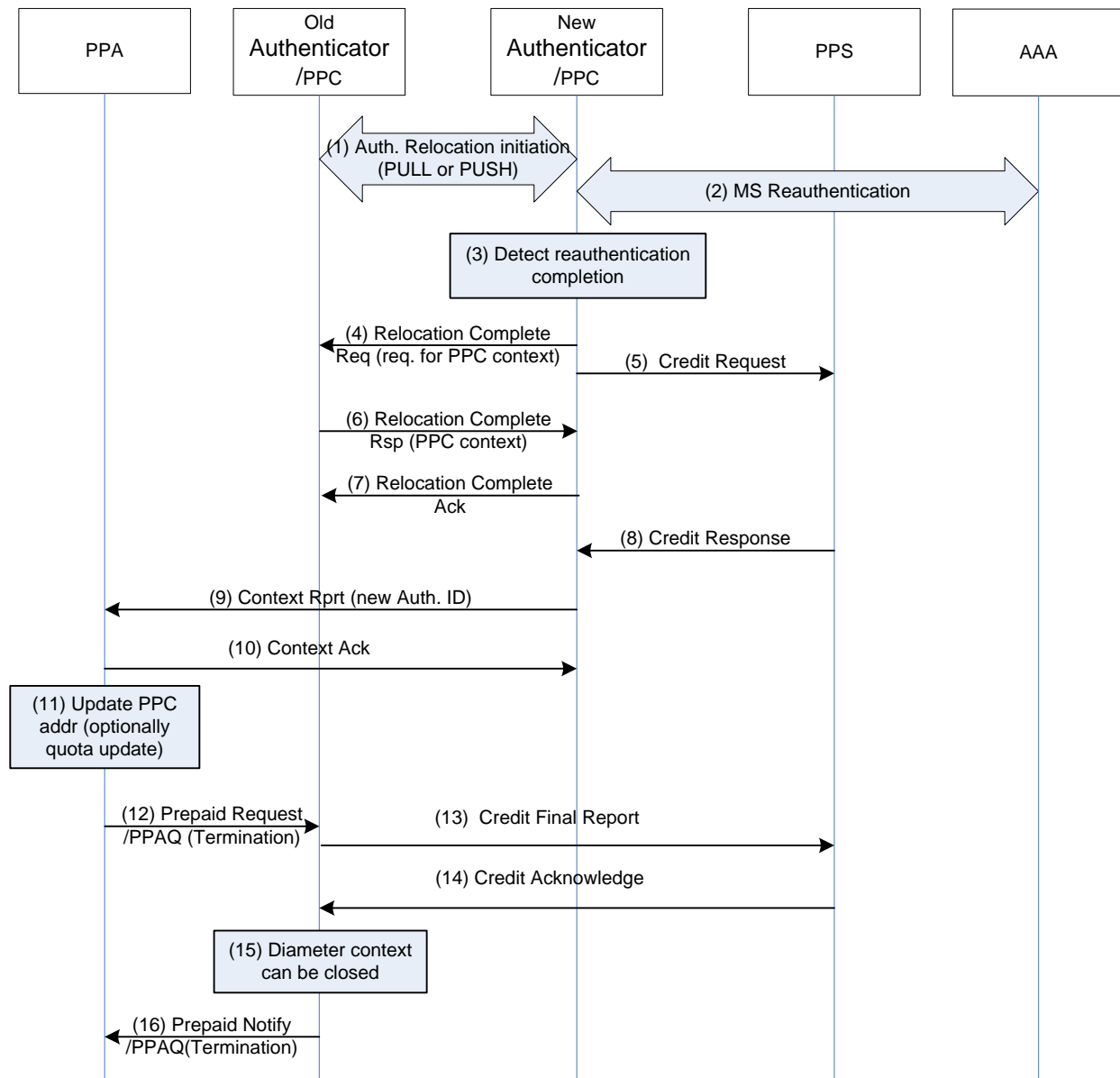
The “old” Authenticator SHALL close the online charging session if the quota exchange was not successful (in case that “new” Authenticator didn’t set the “Online Accounting context” or if the “old” Authenticator didn’t provided the PPC Context).

**STEP 9**

The “new” Authenticator/ PPC/ AAA Client performs accounting update – sends Acct Start for the new accounting segment (session-continue). Acct Start (session-continue) from the “new” Authenticator means authenticator relocation has been successfully completed. If HAAA receives no Acct Start from the “new” Authenticator, it SHALL consider the “old” Authenticator identity (NAS ID) as a PPC (authenticator relocation failed).

**4.4.3.3.6 PPC Relocation in case of Diameter based Online Accounting**

Figure 4-22 shows the case where the location of PPC changes due to Authenticator/PPC relocation. When a new Authenticator is established, a second Diameter Credit Control (DCC) session is established between the new PPC and the PPS. After the relocation finishes, the first DCC session at the old Authenticator between the old PPC and the PPS is torn down. Two DCC sessions exist for some amount of time during the relocation. However at all times, there is only one logical PP-context and credit pool for the user. In this relocation procedure, the PPS can have two different behaviors depending on implementation. In case [a], the PPS continue with the existing PP quota and this quota is transferred from the old DCC session to the new DCC session whereas in case [b], the PPS uses the existing quota on the old DCC session and creates a new quota for the new DCC session. In case [b], a quota is always associated with a single DCC session and never transferred between DCC sessions. In the following description, the differences are marked with paragraphs [a] and [b].



**Figure 4-22 – PPC relocation procedure**

**STEP 1**

Authenticator relocation is initiated (PUSH or PULL modes).

**STEP 2**

MS Re-authentication occurs in the “new” Authenticator entity. This includes EAP Phase and PKMv2 3WHS Phase.

**STEP 3**

In the case the “new” Authenticator detects successful completion of re-authentication process (successful completion of PKMv2 3WHS Phase), it initiates R4 Relocation Complete transaction.

**STEP 4**

The “new” Authenticator informs the “old” Authenticator about the successful completion of re-authentication process by sending Relocation Complete Req message. The “new” Authenticator sets “Online Accounting Context” bit in the Context Purpose Indicator TLV to indicate support for online charging.

**STEP 5**

The “new” Authenticator/PPC SHALL send a Credit Request message indicating A-PCEF relocation to the PPS. The PPS SHALL update the existing PP-context to be associated with both the Diameter Credit Control (DCC) session with the “old” Authenticator/PPC and the DCC session with the “new” Authenticator/PPC. Dependent on the PPS,

[a] The PPS SHALL update the existing PP-context quota related to the DCC session with the “old” PPC to be now associated with the DCC session with the “new” Authenticator/PPC.

[b] The PPS SHALL create a new PP-contextquota associated with the DCC session to the “new” Authenticator/PPC.

**STEP 6**

The “old” Authenticator/PPC responds with Relocation Complete Rsp message providing MS context including PPC Context.

**STEP 7**

The “new” Authenticator/PPC confirms reception of Relocation Complete Rsp message by sending Relocation Complete Ack message. The “old” Authenticator/PPC waits now for prepaid session termination requested by the PPA.

**STEP 8**

Depending on the PPS, option [a] or [b] takes place.

[a] PPS SHALL send a Credit Response (without a new quota) to confirm the credit request.

[b] PPS SHALL return a new quota by sending Credit Response message. The PPC SHALL discard the PPC Context received from the old Authenticator/PPC in step 6.

**STEP 9**

When Relocation Complete Rsp message (Step 6) and Credit Response message (Step 8) are received, the “new” Authenticator/PPC sends Context Rpt message to the PPA to update it with the new Authenticator location/identity.

[a] There is no quota information included the PPA SHOULD continue with the existing one.

[b] In the same message, a new quota SHALL be provided to the PPA. The PPA SHALL use the new quota from this moment on.

From this moment on, the PPA entity SHALL communicate quota updates with the “new” PPC.

**STEP 10**

PPA responds with the Context Ack message.

**STEP 11**

[a] The PPA SHALL update the reference to the new PPC and continue with the existing quota.

[b] The PPA SHALL install the new quota and close the quota related to the old prepaid session. It is required that old and new quotas are managed separately in the PPA. Note: PPA may continue with the old quota if new received quota was zero and would delay sending final report accordingly.

**STEP 12**

- [a] The PPA SHALL trigger the PPC to terminate the old DCC session without returning the used quota.
- [b] The PPA SHALL initiate the termination of the old DCC session indicating used quotas in Used-Service-Unit AVP format.

**STEP 13**

- [a] The “old” PPC SHALL trigger termination of the DCC session by sending the Credit Final Report message in which a final report is not included.
- [b] The “old” PPC SHALL send the Credit Final Report message to PPS and terminate this DCC session.

**STEP 14**

PPS SHALL confirm DCC session termination by the Credit Acknowledge message.

**STEP 15**

The “old” PPC SHALL close the prepaid context.

**STEP 16**

The “old” PPC SHALL inform the PPA that it has closed the old prepaid session.

**4.4.3.3.7 PPA Relocation**

Prepaid Agent (PPA) is collocated with MS’ Anchor DPF/ FA functional entities. When Anchor DPF/ FA relocation scenario occurs, PPA is also relocated. The PMIP4 scenario is presented in the section [4.8.2.3.7]. The CMIP4 scenario is described in [4.8.3.3]. Anchor DPF/FA Relocation also accompanies HLD Relocation, if HLD is collocated with the Anchor DPF/FA and not with the HA. Message remains the same for HLD Relocation; except with the addition of Hot-Lining related TLVs.

The below figure refers a generic Anchor DPF relocation scenario highlighting specifics relevant for PPA relocation.

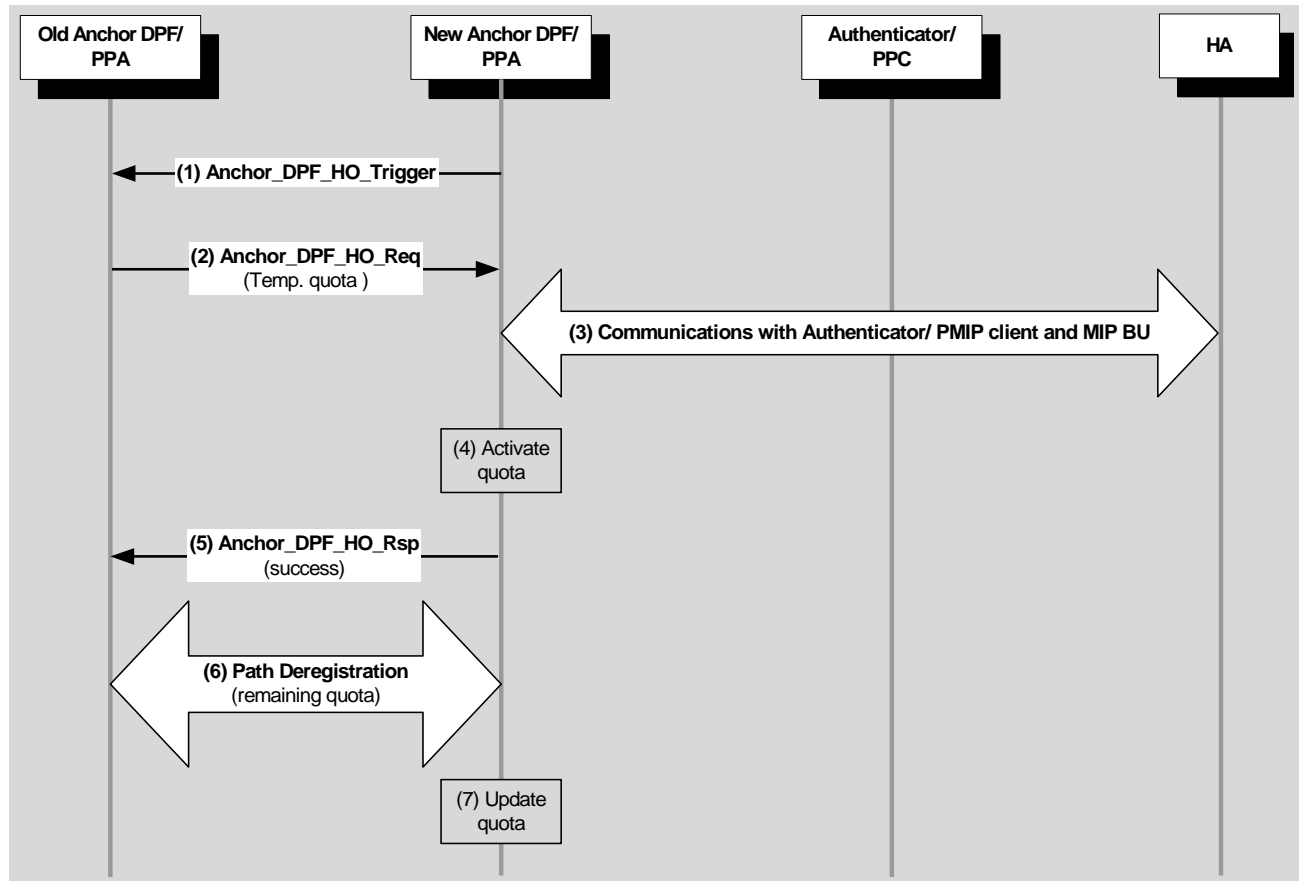


Figure 4-23 – PPA Relocation

### STEP 1

If the Anchor DP relocation trigger occurs in the Target ASN (the “new” Anchor DP), then it instigates Anchor DP HO procedure by sending *Anchor\_DPF\_HO\_Trigger* message to the “old” Anchor DP entity. Otherwise, this step is skipped. The Target ASN should include PPAC TLV to indicate its support for online accounting. If the “old” Anchor DP does not receive PPAC TLV in this step, it SHALL assume that the Target ASN does not support online accounting capabilities. In this case, the “old” Anchor DP SHALL reject Anchor DP/ FA/ PPA relocation.

### STEP 2

Anchor DP HO trigger occurs in the “old” Anchor DP entity. This may be a local trigger or instigated by *Anchor\_DPF\_HO\_Trigger* message from the “new” Anchor DP.

The “old” Anchor DP entity initiates Anchor DPF relocation by sending *Anchor\_DPF\_HO\_Req* message to the “new” Anchor DP.

The “old” PPA should include PPAC TLV in this message to indicate the online accounting capabilities which support is required.

The “old” PPA entity also allocates and includes in this message both expended quota and original quota obtained from PPC before (in PPAQ TLV)– for use by the new PPA when Anchor DP/ FA relocation completes successfully. Handling of expended quota is internal to the respective implementation.

If the Target ASN does not support online accounting capabilities, it SHALL reject Anchor DP/ FA/ PPA relocation.



**STEP 3**

This is a complex step including multiple interactions specific for different scenarios (PMIP4, CMIP4, etc.). As a part of this step, there is MIP binding update occur and the “new” Anchor DP/ PPA updates Authenticator/ PPC with its location/ identity.

For the PMIP4 case this step is represented by steps (3) – (7) on the [Figure 4-122].

In the CMIP case, when CSN-anchored HO is successfully completed, the “new” Anchor DP/PPA sends *Context\_Rpt* message to Authenticator/ PPC including Anchor GW Identity TLV. Authenticator/ PPC receiving this *Context\_Rpt* message updates its notion of the location of Anchor DP/PPA entity and confirms it by sending *Context-Ack* message.

**STEP 4**

When the “new” Anchor DP entity detects the successful MIP binding update completion, it activates the “temporary” quota for user traffic coming from HA. Note, that this SHALL NOT include user traffic, which may still come from the “old” Anchor DP over R4, - to avoid “double counting”.

**STEP 5**

The “new” Anchor DP/ PPA sends *Anchor\_DPF\_HO\_Rsp* message to the “old” Anchor DP/PPA to indicate successful FA relocation.

**STEP 6**

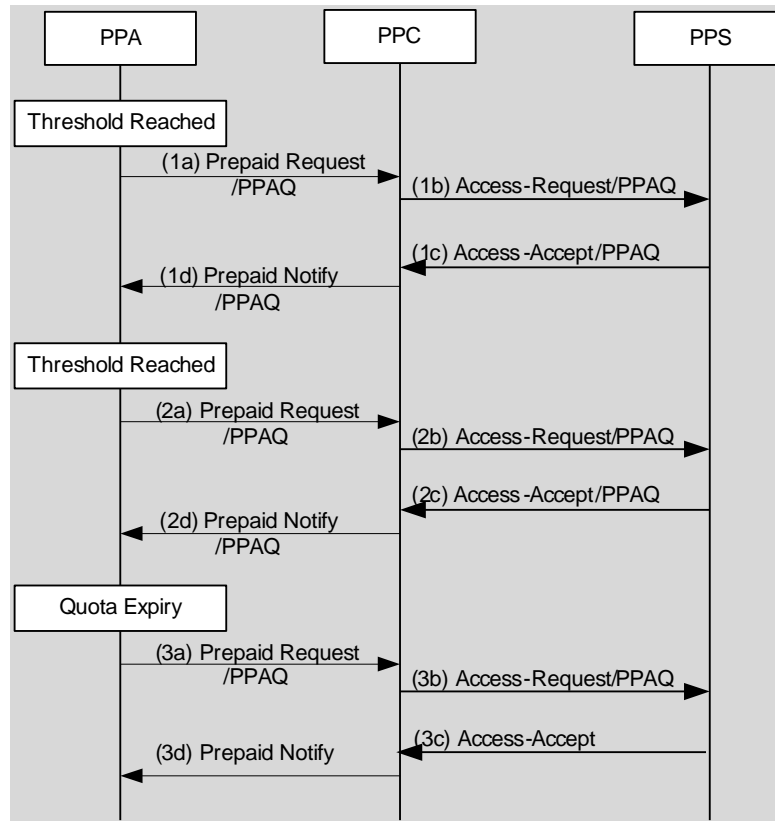
Either “new” or “old” Anchor DP initiates R4 Path Deregistration transaction between them. As a part of this transaction, the “old” PPA provides the expended quota (PPAQ TLV) until now to the “new” PPA for quota correction and finally removes MS context.

**STEP 7**

The “new” PPA updates its quota reserve with the value received from the “old” PPA.

**4.4.3.3.8 PPA-PPC quota(s) update**

PPA communicates online accounting events with PPC (quota updates/ requests) using *Prepaid\_Request* and *Prepaid\_Notify* messages.



**Figure 4-24 – PPA-PPC quota(s) update**

**STEP 1a**

If the threshold of the quota(s) is reached, the PPA requests additional quota by sending a Prepaid Request, containing one or more PPAQ indicating which quota(s) need to be replenished to the PPC.

**STEP 1b**

Upon receiving the Prepaid Request from PPA, PPC sends an Authorize Only Access-Request to PPS for requesting additional quota.

**STEP 1c**

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

**STEP 1d**

The PPC sends Prepaid Notify to the PPA, containing the new quota(s).

**STEP 2a**

Once again a threshold is reached for one or more of the quotas and the PPA requests more quotas by sending a Prepaid Request to the PPC.

**STEP 2b**

Upon receiving the Prepaid Request from PPA, PPC relays the quota request by sending an Authorize-Only Access-Request to the PPS.

**STEP 2c**

The PPS responds with the final quota in the 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 2d**

The PPC sends Prepaid Notify to PPA, containing the new quota(s).

**STEP 3a**

The quota expires. The PPA sends a Prepaid Request packet indicating that the quota has expired. PPA also stops resource allocation for the service.

**STEP 3b**

Upon receiving the Prepaid Request, the PPC sends an Authorize Only Access-Request packet to the PPS indicating that quota has expired.

**STEP 3c**

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

**STEP 3d**

The PPC sends Prepaid Notify to PPA. If there are no additional resources, PPC initiates service termination.

**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 for IP-CS or one ETH-Session for ETH-CS. Each session may have a number of flows. This accounting model is illustrated in Figure 4-17.

According to this model, accounting can be done at two different levels. It can be session-based, or flow-based. In other words, accounting records can be collected per IP-/ETH-session or per 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. Session-based accounting is mandatory to support by the ASN and CSN. 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 flow-based accounting and the CSN chooses session-based accounting, the ASN may report session-based accounting to the CSN by consolidating flow-based accounting records per IP-/ETH-session.

Flow-based accounting has the flexibility to support session-based accounting by providing a mechanism to correlate flow-based accounting records per IP-/ETH-session. The following description applies to both session-based accounting and flow-based accounting. However, if the vendor chooses to implement session-based accounting in the ASN, then the description of flow ID or QoS profile ID becomes irrelevant.

In the context of 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 reported by the SFA.

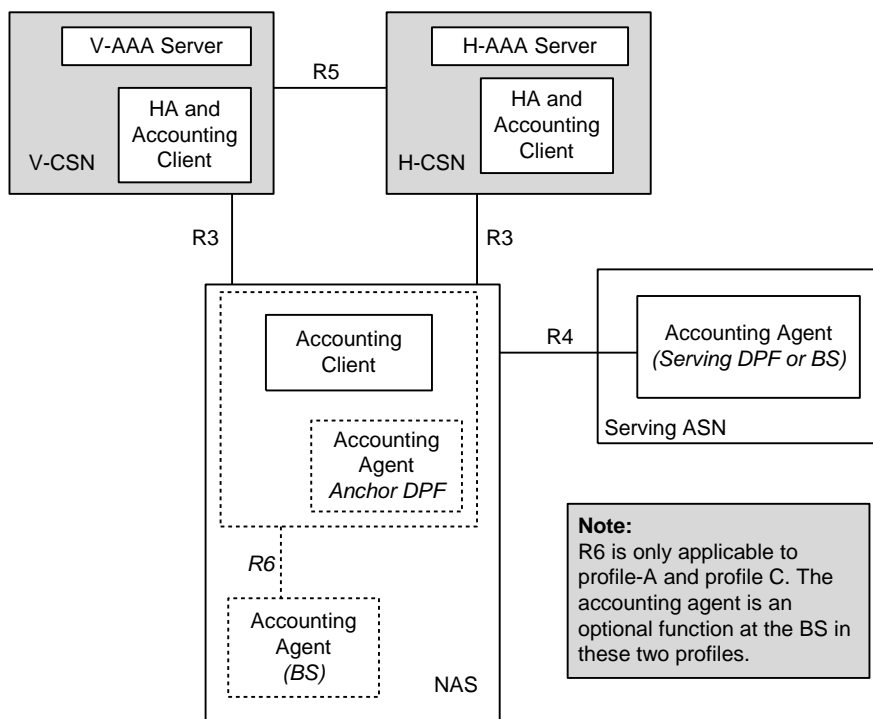
Note that the values of PDFID and SDFID are allocated by CSN entities (e.g., by Home AAA server for the case of preprovisioned flows).

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. Both Volume and Duration Counts SHALL be sent to AAA. 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 uncompressed IP or Ethernet traffic to/from the mobile. When located at the BS, the accounting agent may report byte counts for the dropped frame over the air.

As the MS moves around and changes the BS, the accounting client at the anchor authenticator continues to collect and aggregate accounting information from the new accounting agent. As long as the anchor authenticator does not change, the accounting session remains the same. While the accounting client is at the anchor authenticator, the relationship between accounting client and accounting agent is illustrated in Figure 4-25.



**Figure 4-25 – Accounting Client and Agent**

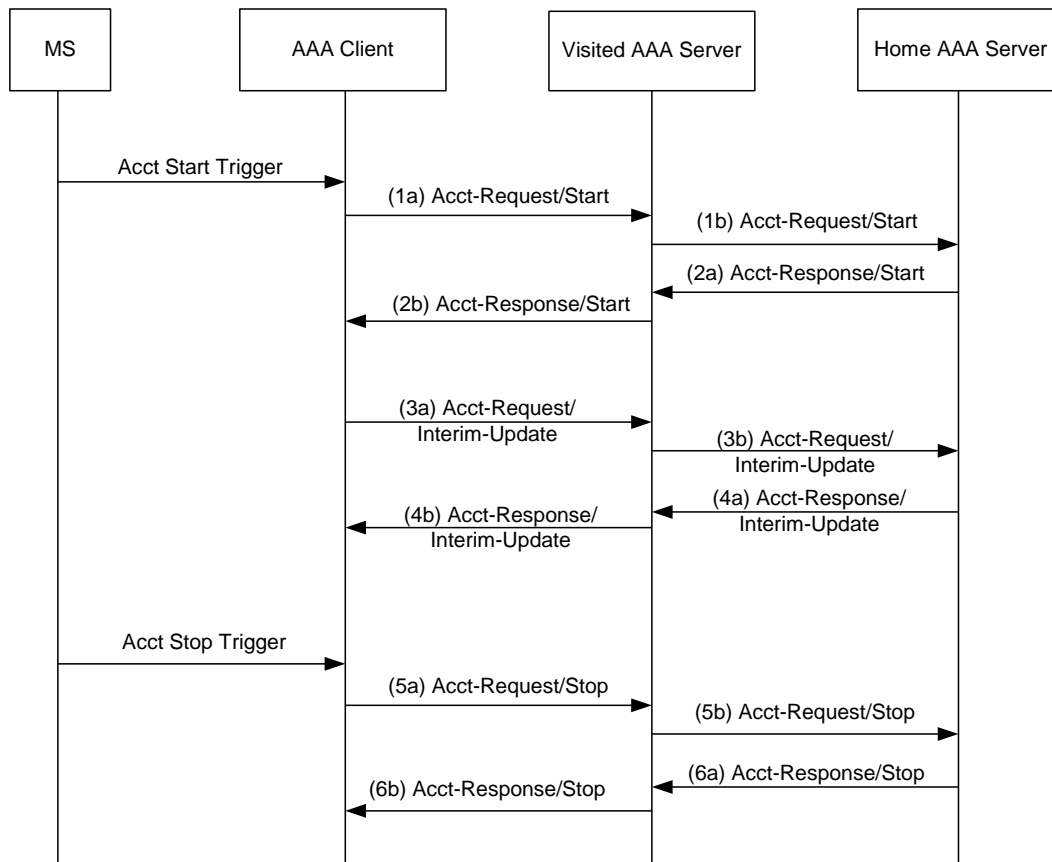
An accounting session is delineated by an Accounting-Request-Start and an Accounting-Request-Stop as per [37] and is identified by the Acct-Session-Id. If flow-based accounting is used, an Accounting Session is established at the creation of each PDFID. If session-based accounting is used, an Accounting Session is established at the time of IP address allocation for IP-CS and at the time of Ethernet ISF establishment for ETH-CS. At the lifetime of a device-session, multiple Accounting Sessions as indicated by Accounting-Starts and Stops may be generated.

Anchored Authenticator (NAS) movement triggers Accounting Segmentation. It generates one or more Accounting Stop messages with the session continue attribute set to true at the old NAS, and one or more Accounting Start messages with the *Beginning-of-Session* attribute set to false at the new NAS. For any other movements like DPF relocation, Accounting Segmentation SHALL NOT occur.

Upon authenticator relocation, the same WiMAX-Session-Id is used for correlating old accounting session with the new accounting session. AAA SHALL send the same WiMAX-Session-Id to the new serving authenticator if the Service-Type is to “Authenticate only” in the RADIUS Access-Request packet or Diameter WDER command.

An Acct-Multi-Session-Id is used to correlate accounting records for multiple service data flows under a session. The Acct-Multi-Session-Id is the WiMAX session id assigned at network access.

Accounting procedures per accounting session are illustrated in Figure 4-26 in case of RADIUS. For Diameter, the same flow with the corresponding messages takes place.



**Figure 4-26 – Offline Accounting Procedures**

In these procedures, the Accounting Client creates independent accounting session for each Packet Data Flow, if flow-based accounting is supported. Packet Data Flow creation causes the ASN to take accounting action. When the accounting client sends a RADIUS Accounting-Request or Diameter WACR message, it SHOULD include the packet data flow information.

#### 4.4.3.4.2 Protocol

WiMAX Release 1.5 is based on RADIUS Accounting as specified by [40] and [38] and [54] in case of Diameter. This specification adds additional requirements to accounting.

##### 4.4.3.4.2.1 Types of Accounting Packets

There are three types of accounting packets:

Accounting Request (Start)

Accounting Request (Interim)

Accounting Request (Stop)

Accounting-Request (Start) packets are mandatory to implement for the accounting client. It signals the beginning of an IP-/ETH-session or a PD-flow.

In Diameter these correspond to Accounting-Record-Type values of START-RECORD, INTERIM-RECORD and STOP-RECORD. WiMAX does not use EVENT-RECORD.

Accounting-Request (Interim) packets are optional to implement for the Accounting Clients. These packets are used to periodically report accounting for the IP-/ETH-session of the PD-flow. The purpose of Interim records is to mitigate revenue loss due to a loss of a stop record. The HAAA controls the Accounting Interim rate by specifying

the number of seconds between Accounting Request (Interim) packets in the Acct-Interim-Interval(85) [40] which is sent in the RADIUS Access-Accept packet to the ASN and optionally to the HA, or Diameter WDEA command to the ASN or optionally the WHAA command to the HA. In the absence of this attribute, the interval between Accounting-Request (Interim) packets is chosen by the accounting client.

Accounting-Request (Stop) packets are mandatory to implement for the accounting client. This information represents the final count for the IP-/ETH-session of the flow.

Each Accounting Start/Stop packet delineates a complete IP-/ETH-session or a flow or a segment of an IP-/ETH-session. An IP-/ETH-session or a flow may consist of several accounting segments. Accounting segmentation occurs due to:

- Accounting client relocation caused by anchored authenticator movement.
- Change in Status such as hot-line state.
- Change in QoS properties for flow

The accounting attributes/AVP Beginning-of-Session, and Session-Continue help in the interpretation of the Accounting-Request packets as shown in Table 4-29.

**Table 4-29 – 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-/ETH-session or a flow.
Start	FALSE (or missing)	N/A	Beginning of a subsequent accounting segment of an IP-/ETH-session or a 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-/ETH-session or the flow.

#### 4.4.3.4.2.2 Transmission and Reception of Accounting Messages

RADIUS supports two types of accounting record transmission. In the pass through style, the forwarding server (RADIUS proxy) forwards accounting messages as soon as it receives the packet, or in batch style where it acknowledges the reception of an accounting message and forwards it later.

WiMAX RADIUS proxies (between the accounting client and the Home CSN) SHALL act in a "pass through" style as defined by [38].

In the case of Diameter three modes of operations are supported as defined by the Accounting-Realtime-Required AVP [54]. The default value of the Accounting-Realtime-Required AVP is “GRANT AND STORE” which means service is provided to the MS as long as you can deliver accounting UDRs or alternatively they can be stored (and delivered later). As per the Diameter specification the AAA can send the Accounting-Realtime-Required AVP back in an WDEA command to the ASN-GW or to the HA in the WHAA command. As well, Diameter allows this attribute to be sent back in the Accounting Answer command thus allowing the Diameter Server to modify the behavior mid-stream.

Care must be taken when setting this attribute. Since many features require that the AAA infrastructure knows the IP address assigned to the session (for example OTA features), then Accounting-Realtime-Required needs to be set to “DELIVER-AND-GRANT”. Note that Accounting-Realtime-Required AVP set to “GRANT-AND-LOSE” means that service can be granted without having an accounting stream and thus may jeopardize billing and auditing.

As the UDRs are transported over the AAA infrastructure they may be routed through proxy servers in the Visited CSN and in other broker networks. These entities may capture the accounting stream and use it to reconcile billing with their partners and also for auditing purposes. The entities should not modify the accounting stream.

Unless otherwise specified, accounting messages do not have to follow the same path as the authentication messages. The routing path of accounting packets is a matter of business agreement between ASN and CSN providers.

#### 4.4.3.4.3 Accounting Information Collection and UDR Structure

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

- 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 5.3.2.373.
- The Anchor/Serving DPF which reports signaling and user data packets and octet counts to/from the mobile. The Anchor/Serving DPF reports separate counts for signaling, user data.

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.

UDR records conform to the RADIUS packet structure as defined by [38] and [40] as well as to [54] in case of Diameter. The payload of the record is defined by WiMAX and is divided into logical blocks as follows.

**Table 4-30 – 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/ETH 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 identify 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.

Each section contains one or more attributes that are defined by RFCs, and attributes specific to WiMAX. WiMAX vendors may add additional attributes as required by specific deployments.

Some of the attributes are required and some are conditionally required or they are optional. The attributes defined by WiMAX are specified in section 5.3.2.373.

#### 4.4.3.4.4 Procedures

##### 4.4.3.4.4.1 Accounting Mode Selection

During Network Access Authentication and Authorization, the NAS SHALL indicate what type of accounting it SHALL be able to support using the WiMAX-Capability attribute that is sent in the RADIUS Access-Request or Diameter WDER command. If the NAS is able to support session-based accounting it SHALL set the session-



based-Accounting bit and if it supports Flow-based accounting for IP-CS it SHALL set the Flow-based-Accounting bit for IP. If the NAS is able to support flow-based accounting for ETH-CS, it SHALL set the Flow-based accounting bit for ETH. The NAS SHALL at least support session-based accounting.

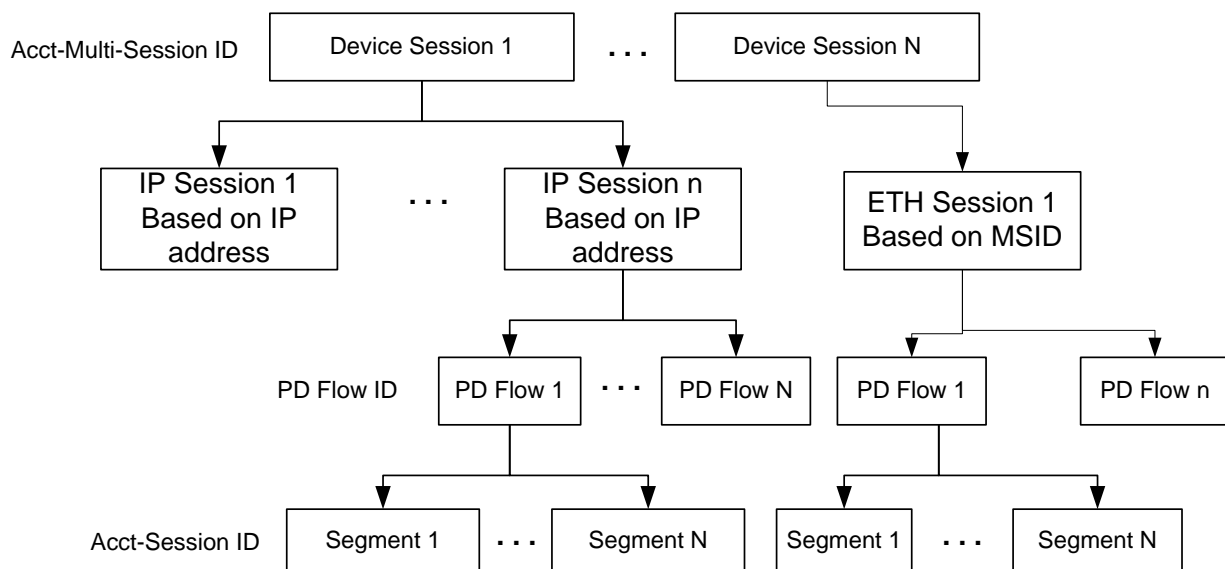
The HAAA server SHALL indicate the mode of accounting to apply to the MS. The HAAA server selects session-based accounting by setting the session-based-Accounting bit in the WiMAX-Capability attribute sent back in the RADIUS Access-Accept packet or Diameter WDEA command. The HAAA server selects flow-based accounting for IP-CS/ETH-CS by setting the Flow-based-Accounting bit for IP/ETH respectively in the WiMAX-Capability attribute sent back in the RADIUS Access-Accept packet or Diameter WDEA command. The HAAA SHALL select one and only one of the accounting modes for a given session or flow.

If the NAS receives an RADIUS Access-Accept or Diameter WDEA command in which the HAAA did not select an accounting mode, or in which the HAAA selected an accounting mode that is not supported by the NAS (as indicated in the RADIUS Access-Request or Diameter WDER command) or conflicts with the CS type, the NAS SHALL treat the RADIUS Access-Accept (Diameter WDEA command) as an Access-Reject (Diameter WDEA command indicating failure) and it SHALL not provide any service to the MS.

#### 4.4.3.4.2 Accounting Record Correlation

The record correlators in the accounting record provide correlation identifiers that support accounting record correlation at different levels in the correlation hierarchy.

Figure 4-27 illustrates the correlation hierarchy and the correlation identifiers associated with each level of correlation.



**Figure 4-27 – Correlation Hierarchy**

Different identifiers are used for correlation at different levels. The Acct-Multi-Session ID correlates accounting records for a device session on a particular device for a given subscription. The IP address correlates accounting records for an IP session on a given device session. The MSID correlates accounting records for an ETH session on a given device session. PD Flow ID correlates accounting records for a PD flow. The Acct-Session ID is used to match accounting Start/Interim/Stop messages for an accounting record on an accounting segment. The Acc-Multi-Session ID is generated by AAA server. The IP address is the home address assigned to the MS. The Packet Data Flow ID is also generated by the AAA server. Generation is described in the QoS section. And finally, the Acct-Session ID is generated by the accounting client.

Note: The NAI is not used as a record correlator, as it may be a pseudonym that is only meaningful to the AAA server and the MS. The AAA server, however, can use the (outer) NAI to correlate a device session to the

subscription and subscriber. This can also be used to relate different device sessions of the same subscription in the AAA server. Also, the CUI can be used by the visited CSN to do record correlation.

#### **4.4.3.4.4.3 Idle Mode Notification**

The anchor authenticator knows when an MS enters or exits the idle mode. (See Section “Idle Mode Entry” and “Idle Mode Exit”). The accounting client collocated at the anchor authenticator may notify the accounting server at the CSN of the idle mode transition using the accounting messages.

Idle mode notification can be negotiated at network access. During network access, the ASN SHALL indicate if it supports idle mode notification using the Idle Mode Notification TLV in the WiMAX-Capability attribute in the RADIUS Access-Request or Diameter WDER command. The HAAA SHALL indicate if it requires idle mode notification using the same TLV in the RADIUS Access-Accept or Diameter WDEA command.

If idle mode notification is supported at the ASN and is required by the CSN, the accounting client at the ASN SHALL send an accounting interim update message with the Idle-Mode-Transition attribute when the MS enters or exits the idle mode. The accounting client at the ASN need not send an accounting interim update message while the MS is in idle mode. The ASN SHALL only send an idle mode notification against the ISF and the message MAY include counters.

#### **4.4.3.4.5 Tariff Switching**

Tariff switching with both the volume and duration based prepaid services are initiated at the Home AAA server.

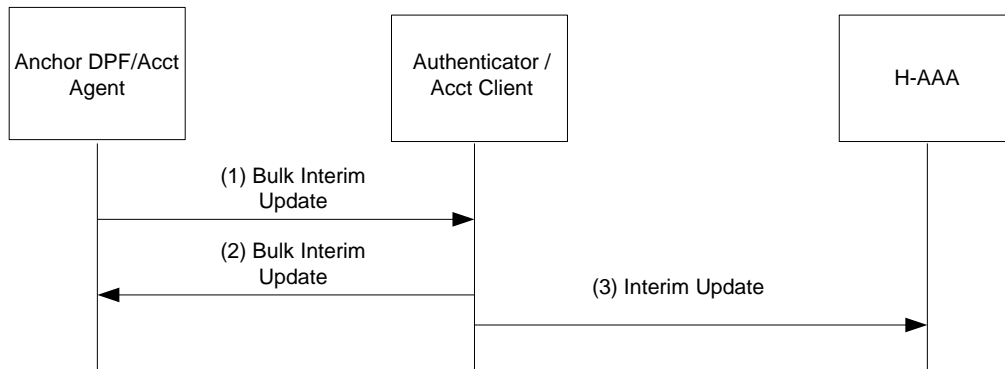
In order to avoid a flood of messages over R6 from BS to ASN-GW at the Tariff Switch Time of Day (ToD) and another flood of messages over R3 from ASN-GW to AAA for all of the AAA messages trigger by the Tariff Switch, optional Tariff Switch attributes have been added the TLVs and messages described below.

- The Accounting Agent saves off the volume counts for a subscriber at the ToD time. When the next accounting event/trigger happens for the subscriber those volume counts at ToD are sent to the Accounting Client along with the regular volume counts. The Accounting Client then generates an Accounting Stop message to capture the accounting information before the ToD and an Accounting Start message to indicate the start of accounting after the ToD. Then the regular AAA message(s) are sent based on event/trigger mentioned above. The AAA messages that include the volume counts at ToD are backdated to the actual time of the ToD for accurate billing.

#### **4.4.3.4.6 Accounting R4 Messaging**

When the Accounting Agent (always co-located with the Anchor DPF) and Accounting Client (always co-located with the Anchor Authenticator) are not co-located, R4 messaging between the two entities is necessary. This section describes the conditions that trigger the messaging.

#### 4.4.3.4.6.1 Bulk Interim Update



**Figure 4-28 – Bulk Interim Update Procedure**

#### STEP 1

When the Interim Update timer expires in the Accounting Agent, the volume counts are collected and sent to the Accounting Client in the BulkInterimUpdate message using the Accounting Bulk Session/Flow Volume Counts TLV. The BulkInterimUpdate message may contain information for one or more subscribers. Volume counts from different subscribers may be gathered in an R4 Bulk Interim Update message if their corresponding "Interim Update Interval"s expire at the same time at the Accounting Agent side.

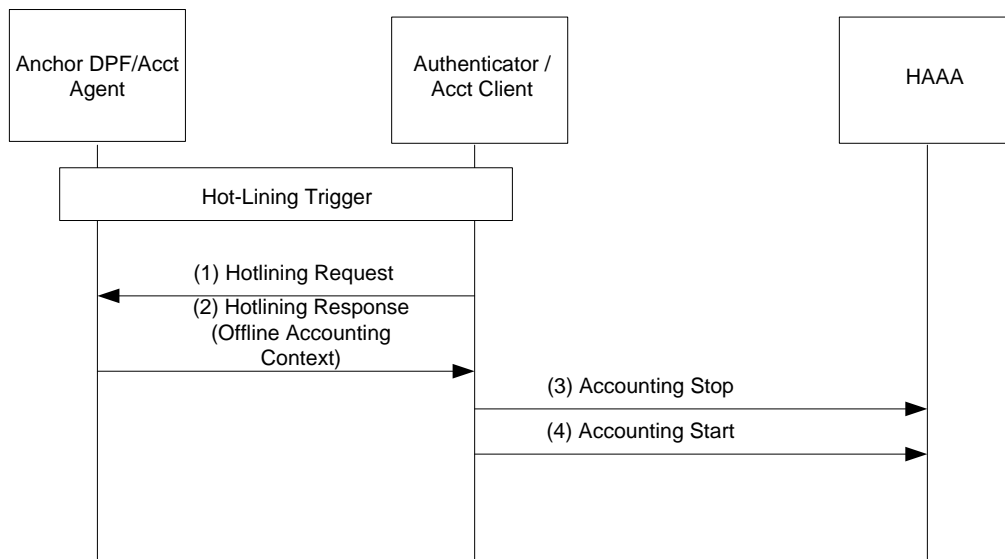
#### STEP 2

The Accounting Client receives the BulkInterimUpdate message and responds with a BulkInterimUpdateAck message.

#### STEP 3

The Accounting Client sends Interim UDR(s) to the HAAA.

#### 4.4.3.4.6.2 Hot-Lining



**Figure 4-29 – Hot-Lining**

#### STEP 1

When a subscriber is hotlined or un-hotlined, the Accounting Client needs to know the offline accounting context (volume counts) at that transition. In this case it requests this from the Accounting Agent over R4 using the Context request message.

#### STEP 2

The Accounting Agent receives the Hotlining Req message and responds with a Hotlining response message which contains the requested context information.

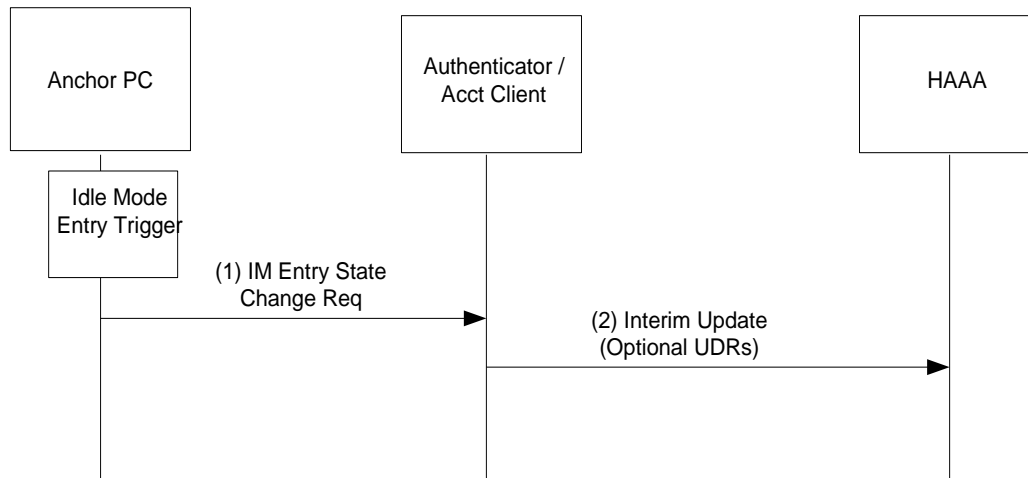
#### STEP 3

The Accounting Client sends Stop UDR(s) (with Session-Continue set to True and Hotlining-Indicator set appropriately) to the HAAA to capture the volume counts at the Hot-Lining transition.

#### STEP 4

The Accounting Client also sends Start UDR(s) (with Beginning-of-Session set to False and Hotlining-Indicator set appropriately) to the HAAA at the Hot-Lining transition.

#### 4.4.3.4.6.3 Idle Mode Entry



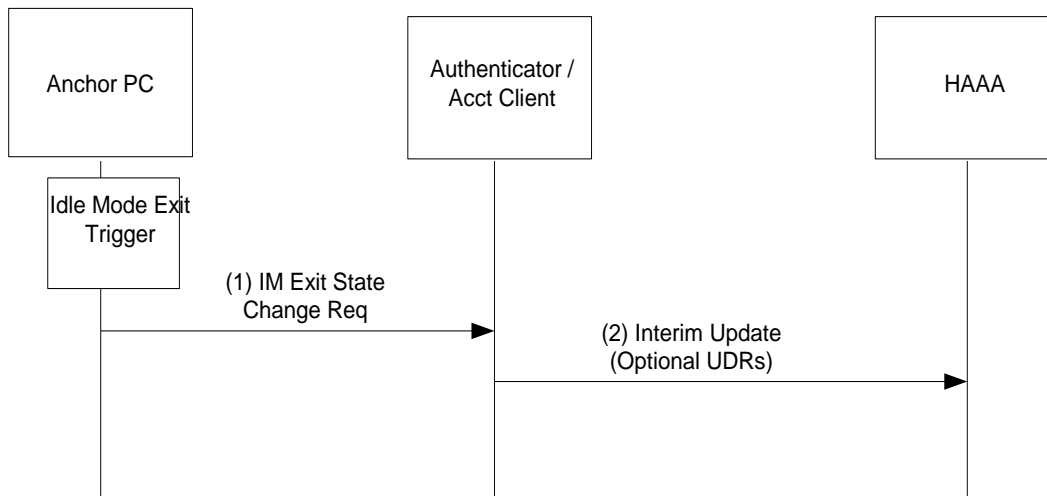
**Figure 4-30 – Idle Mode Entry**

**STEP 1**

During Idle Mode Entry, the Anchor PC/LR sends the IM Entry State Change req message to the Authenticator/Accounting Client. The Accounting Agent is responsible for keeping track of the cumulative counts when the user enters idle mode.

**STEP 2**

The Accounting Client sends optional (only if Idle-Mode-Notification is turned on) Interim UDR(s) to the HAAA.



**Figure 4-31 – Idle Mode Exit**

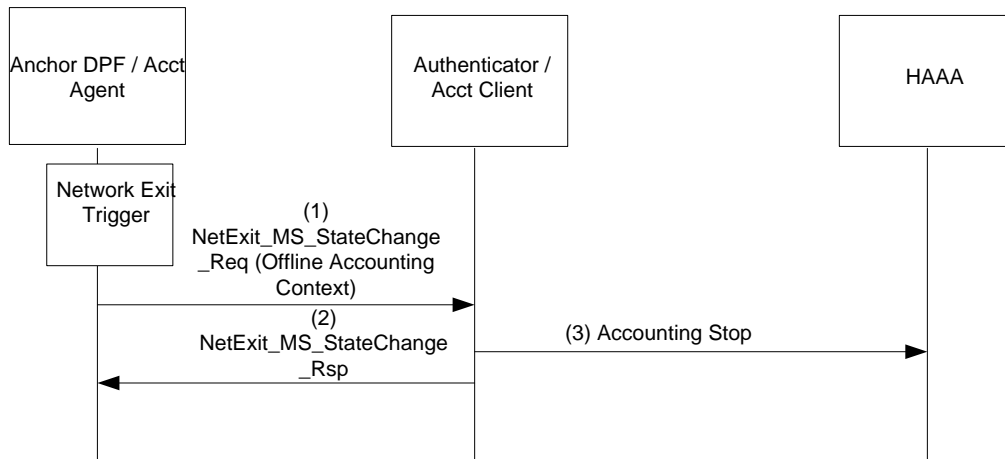
**STEP 1**

During Idle Mode Exit, the Anchor PC/LR sends the IM Exit State Change req message to the Authenticator/Accounting Client.

**STEP 2**

The Accounting Client sends optional (only if Idle-Mode-Notification is turned on) Interim UDR(s) to the HAAA.

#### 4.4.3.4.6.4 Network Exit



**Figure 4-32 – Network Exit**

#### STEP 1

During Network Exit (this is triggered by the Path\_Dereg\_Req message), the Accounting Agent collects the final volume counts and sends them to the Authenticator/ Accounting Client in the NetExit\_MS\_State\_Change\_Req message using the Accounting Bulk Session/Flow Volume Counts TLV.

#### STEP 2

The Authenticator/ Accounting Client receives the NetExit\_MS\_State\_Change\_Req message and responds with a NetExit\_MS\_State\_Change\_Rsp message.

#### STEP 3

The Accounting Client sends final Stop UDR(s) to the HAAA.

#### 4.4.3.4.7 Accounting Client Relocation

Accounting Client is collocated with MS' Authenticator entity. During Authenticator relocation scenario described in the section [4.4.1.5.5.2], the Accounting Client is also relocated. Accounting Client relocation procedure described here is applicable only for PMIP and CMIP.

The Accounting Client always gets the cumulative volume counts from the Accounting Agent. This means that the Accounting Client does not keep a master copy of the volume counts and will simply include the counts from the Accounting Agent in the UDR. The Accounting Client keeps track of duration counts, so those need to be transferred during Accounting Client relocation.

The below figure describes the specifics relevant for Accounting Client relocation.

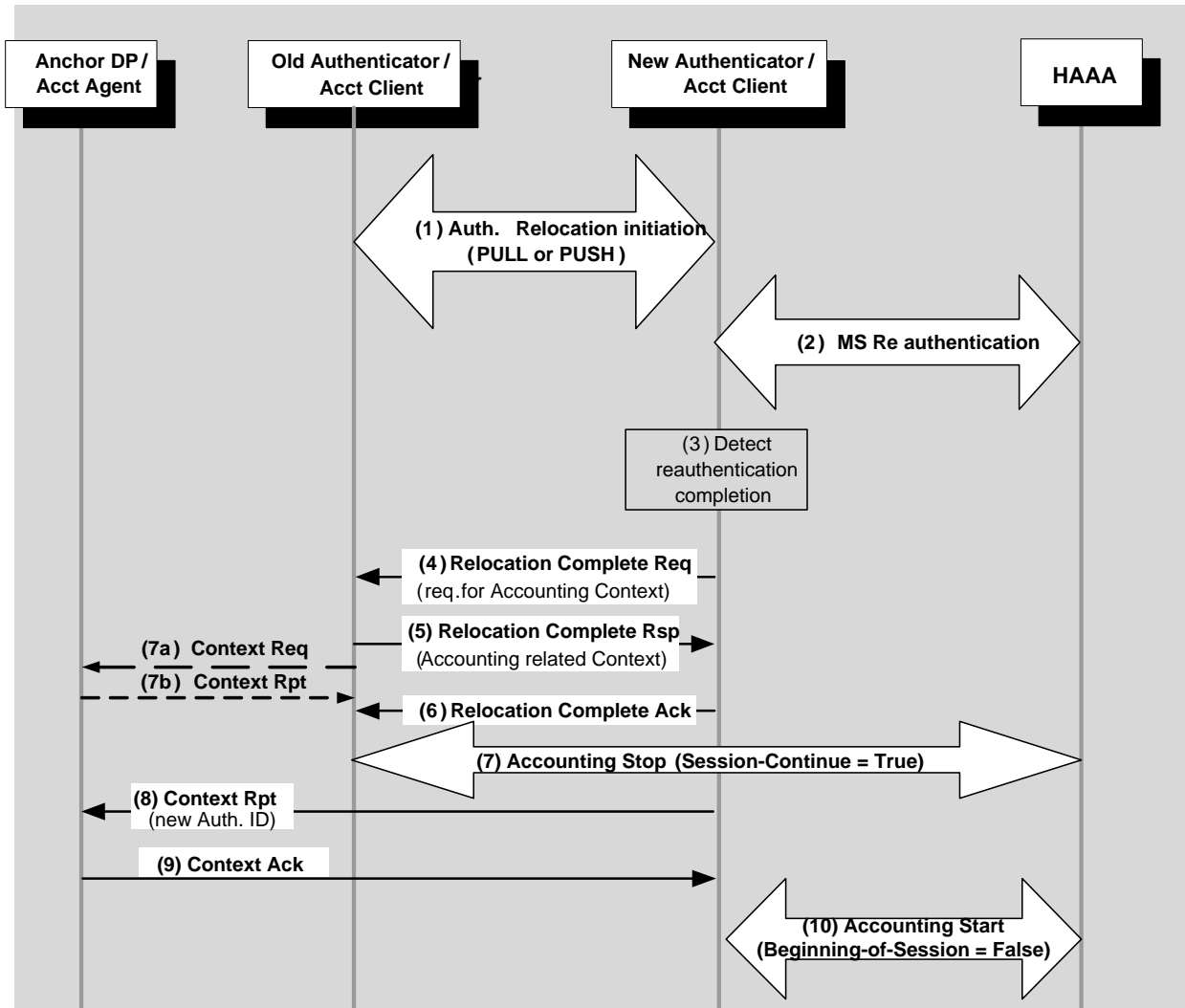


Figure 4-33 – Accounting Client relocation

### STEP 1

Authenticator relocation is initiated (PUSH or PULL modes).

### STEP 2

MS Reauthentication occurs in the “new” Authenticator entity. This includes EAP Phase and PKMv2 3WHS Phase.

### STEP 3

In the case the “new” Authenticator detects successful completion of reauthentication process (successful completion of PKMv2 3WHS Phase), it initiates R4 Relocation Complete transaction.

### STEP 4

The “new” Authenticator informs the “old” Authenticator about the successful completion of reauthentication process by sending *Relocation\_Complete\_Req* message. The “new” Authenticator sets the “Accounting context” bit in the Context Purpose Indicator TLV to indicate the request for the Accounting context.

## STEP 5

The “old” Authenticator responds with *Relocation\_Complete\_Rsp* message providing MS context including the Accounting Context with the duration counts.

## STEP 6

The “new” Authenticator confirms reception of *Relocation\_Complete\_Rsp* message by sending *Relocation\_Complete\_Ack*. When the “old” Authenticator receives this message it may delete MS context.

**Table 4-31 – Context\_Rpt from Accounting Agent to “Old” Accounting Client**

IE	Reference	M/O	Notes
Offline Accounting Context	5.3.2.360	M	
>Accounting Bulk Session/Flow Volume Counts	5.3.2.359	M	
>>Accounting Number of Bulk Sessions	5.3.2.245	M	
>>Accounting Bulk Session/Flow	5.3.2.246	M	
>>>SFID	5.3.2.184	O	
>>>Accounting IP Address	5.3.2.264	M	
>>>Accounting Session/Flow Volume Counts	5.3.2.244	M	
>>>>Cumulative Uplink Octets	5.3.2.249	M	
>>>>Cumulative Downlink Octets	5.3.2.250	M	
>>>>Cumulative Uplink Packets	5.3.2.251	M	
>>>>Cumulative Downlink Packets	5.3.2.252	M	
>>>>Uplink Octets at Tariff Switch	5.3.2.257	O	
>>>>Downlink Octets at Tariff Switch	5.3.2.258	O	
>>>>Uplink Packets at Tariff Switch	5.3.2.259	O	
>>>>Downlink Packets at Tariff Switch	5.3.2.260	O	

## STEP 7

The “old” Authenticator/Accounting Client may initiate a context retrieval procedure with the Accounting Agent in order to retrieve the volume counts by setting the offline accounting context bit in the context request message.

The “old” Authenticator/ Accounting Client generates a Stop UDR (with Session-Continue flag set to true) for the previous accounting segment.



**STEP 8**

The “new” Authenticator/ Accounting Client sends *Context\_Rpt* message to the Anchor DP/ Accounting Agent to update it with the new Authenticator location/ identity. From this moment, the Accounting Agent entity will communicate accounting updates with the “new” Accounting Client.

**STEP 9**

Anchor DP responds with *Context-Ack* message.

**STEP 10**

The “new” Authenticator/ Accounting Client generates a Start UDR (with Beginning-of-Session flag set to false) for the new accounting segment. A Start UDR from the “new” Authenticator means authenticator relocation has been successfully completed. If HAAA does not receive a Start UDR from the “new” Authenticator, it SHALL consider the “old” Authenticator identity (NAS ID) as the Accounting Client (authenticator relocation failed).

**4.4.3.5 Hot-lining**

As indicated in NWG Stage-2 document, the Hot-lining feature provides a WiMAX operator with the capability to efficiently address issues with the users that would otherwise be unauthorized to access packet data services. The hot-lining device (HLD) can be at the ASN, or located at the CSN. As discussed in NWG Stage-2 document, there are two methods defined by which the HAAA indicates that a user is to be hot-lined:

- Profile based Hot-lining: For the profile based Hot-lining, Hot-line profile(s) with all Hot-lining rules are pre-provisioned at the HAAA. The HAAA sends a hot-line profile identifier in the RADIUS message (Access-Accept and Change of Authorization) when the Hot-lining is activated.
- Rule based Hot-lining: Hot-lining rules (filter rules, IP or HTTP redirection rules) are sent in the RADIUS message (Access-Accept and Change of Authorization) by the HAAA when the Hot-lining is activated.

Based on the status of the user’s session, there are two ways users can be hot-lined,

- Active Session Hot-lining: The user starts normal packet data session and in the middle of the session, the HAAA receives trigger for Hot-lining from the Hot-lining Application (HLA).
- New Session Hot Lining: The trigger from the HLA arrives prior to the user access authentication.

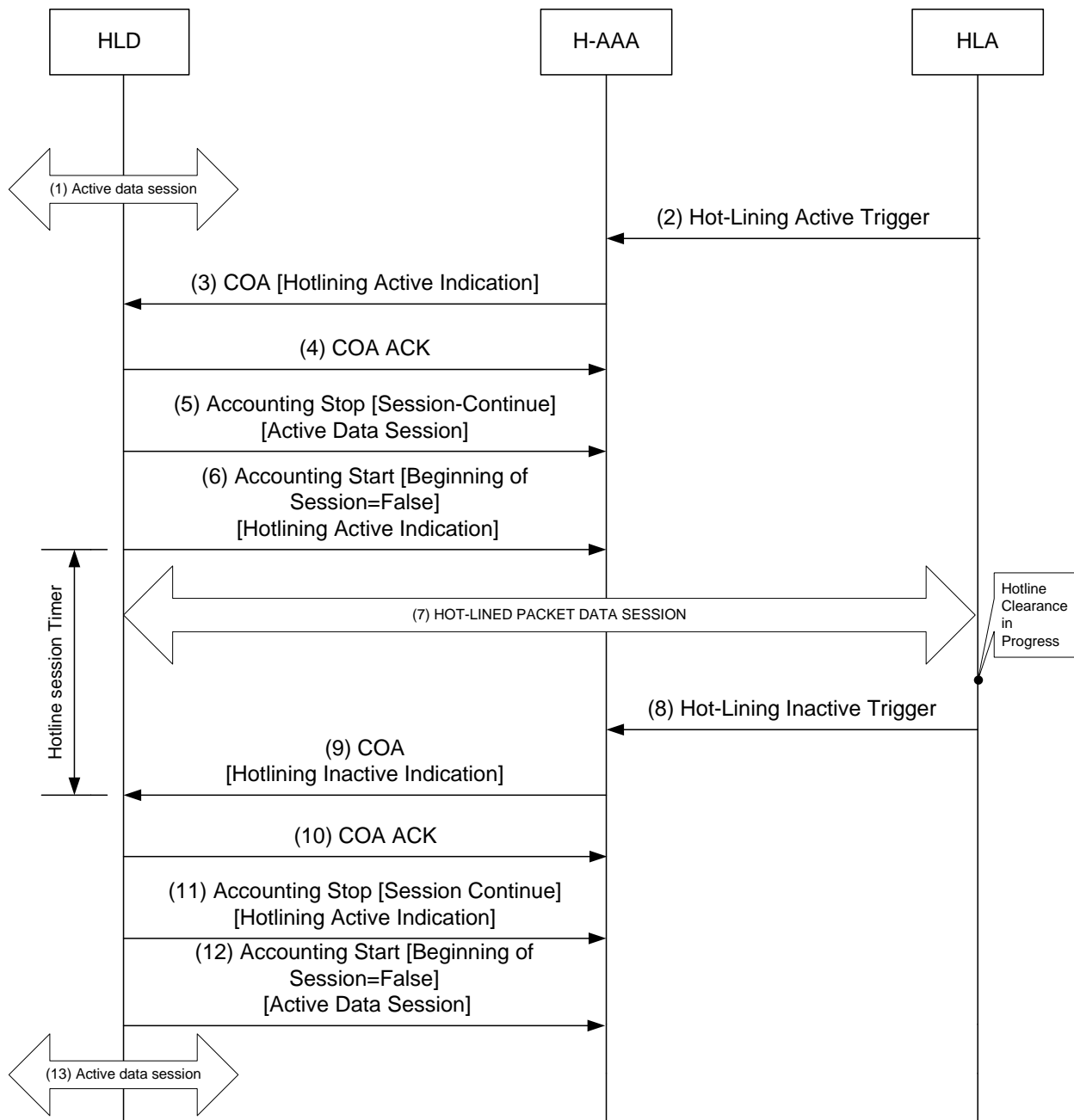
Once the hot-lining is resolved, the packet data session is returned to normal. Both these approaches are discussed in the following sub-sections.

Only IP session based Hot-Lining procedures are defined in this document. PD flow based Hot-Lining may be defined in the future version of this document.

Note: Hot-Lining for Diameter based Online Charging is current out of scope and will be provided in a later release.

**4.4.3.5.1 Active Session Hot-lining**

The active IP session hot-lining is invoked when the user is currently engaged in a packet data session and the HAAA receives hot lining trigger from the HLA. Figure 4-34 depicts the call flow between the HLD, HAAA and HLA.



**Figure 4-34 – 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 of the current Release.

**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 Hotlining request to the HLD or it may send a RADIUS Disconnect Message (DM) to the HLD for terminating the session.

**STEP 5**

The HLD sends a RADIUS Accounting Request (Stop) indication for the active data session, with Session Continue set to true.

**STEP 6**

The HLD sends RADIUS Accounting Request (Start) for the hot-lined session with *Beginning-of-Session* set to False. If Session-Timeout attribute was included in step 3, the HLD initiates session teardown (i.e., tear down of the service flows associated with the IP session) when the duration specified in the Session-Timeout attribute has elapsed and the user's session is still hot-lined. After tearing down the service flow(s), the HLD sends an Accounting Request (Stop) to the HAAA to inform that the user's IP session has ended.

**STEP 7**

Since the user's data session is hot-lined in mid session, user's data traffic is affected. Based on the Hot-lining rules set at the HAAA and indicated by it in the RADIUS COA earlier, the uplink and/or downlink data traffic of the user is either dropped/disconnected, or blocked, and redirected to the HLA by the HLD.

**STEP 8**

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 resolve the issue. The method of notification to the user is undefined in this document.

- If the condition which triggered the hot-lining session does not get cleared, the HLA may terminate the session. In this case, the HAAA is notified by the HLA. Upon receipt of this notification, the HAAA SHALL send a RADIUS Disconnect Message to the HLD where the accounting records are stopped and the session termination is initiated. This may also happen automatically at the HLD, if the user's Hot-Lined status does not change within the duration of the Session-Timeout value.
- Otherwise, if the condition that triggered Hot-lining session gets cleared (via an undefined procedure), the HLA detects this and indicates to the HAAA to clear the Hot-lined status of the user by sending the Hot-lining Inactive Trigger to the HAAA.

**STEP 9**

Upon receipt of the Hot-lining Inactive Trigger, the HAAA sends a RADIUS COA message to the HLD with appropriate attributes. Note that this may not be the same HLD that initially handled the activation of the Hot-lining. This may occur due to events like handoff.

**STEP 10**

Upon receipt of the RADIUS COA:

- If the HLD can honor the request then it will respond with a RADIUS COA Ack to the HAAA and Hot-line Session-Timeout timer is turned off.
- If the HLD cannot honor the request then it SHALL respond with a COA NAK message. Based on the local policy, the HAAA may either retry sending the Hot-Lining signal to the HLD or it may send a RADIUS Disconnect Message to the HLD for terminating the session. In this case, the HLD sends a RADIUS Accounting Request (Stop) message to the HAAA indicating the end of the IP session for the user after it successfully processed the Disconnect Message and tears down the service flow(s) associated with the IP session.

**STEP 11**

The HLD generates RADIUS Accounting Request (Stop) with Session Continue set to True message for the hot-lined packet data session.

**STEP 12**

The HAAA sends a RADIUS Accounting Request (Start) message with *Beginning-of-Session* set to False indicating the start of the normal packet data session.

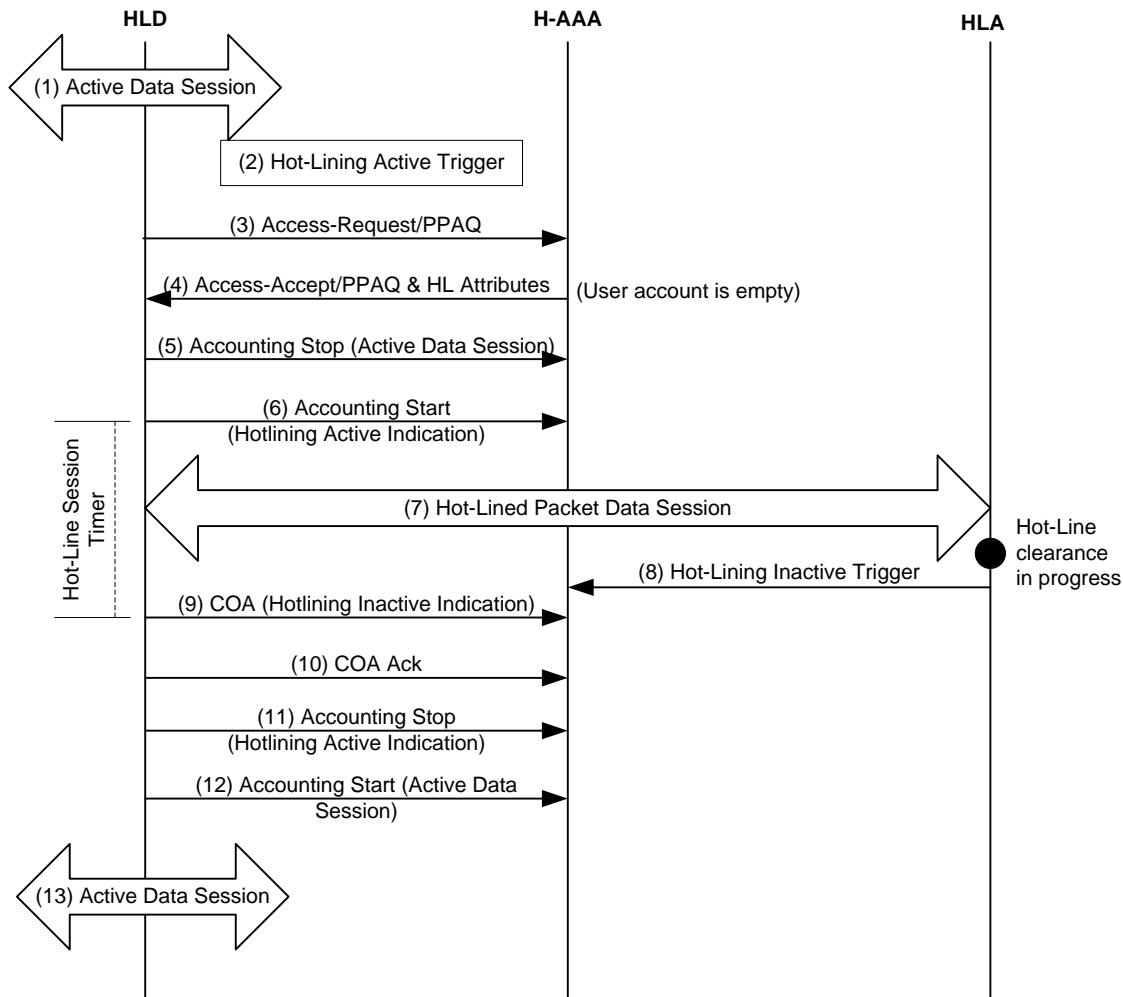
**STEP 13**

User continues the packet data session and the traffic is routed normally.

During the Hot-Lined active status in the HLD, the byte, packet and duration counts for user's hot-lined IP session MAY be counted towards the overall byte and packet counts. In this document, the byte/packet counts during Hot-Line active status are not reported to the accounting server by the accounting client.

**4.4.3.5.1.1 Active Session Hot-lining for Prepaid**

Active IP session hot-lining MAY also be invoked when the prepaid user is currently engaged in a packet data session and the HAAA /PPS does not grant additional quota to the user. Figure 4-25 depicts the call flow between HLD/PPC, HAAA/PPS and HLA.



**Figure 4-35 – Active IP Session Hot-lining for prepaid user account replenishment**

**STEP 1**

Prepaid user is in an active IP session that is not Hot-lined.

**STEP 2**

The threshold for the prepaid quota(s) is reached.

**STEP 3**

PPC requests additional quota by sending an Authorize-Only Access-Request, containing one or more PPAQ indicating which quota(s) need to be replenished to the PPS (assumed to be collocated with HAAA).

**STEP 4**

PPS responds back with an Access-Accept packet. The balance on the user account is too low for additional quota to be allocated. Hot-lining is triggered for the user to replenish his/her account. Access-Accept is sent 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. PPAQ/Termination-Action is set to Redirect/Filter.

## STEP 5

From this point on all steps are identical to those of figure 4-24.

### 4.4.3.5.2 New IP Session Hot-lining

New IP session Hot-lining is invoked when the user starts a new IP session and the HAAA already has Hot-lining status set for that IP session for that user. Figure 4-36 depicts the call flow between the HLD, HAAA and HLA.

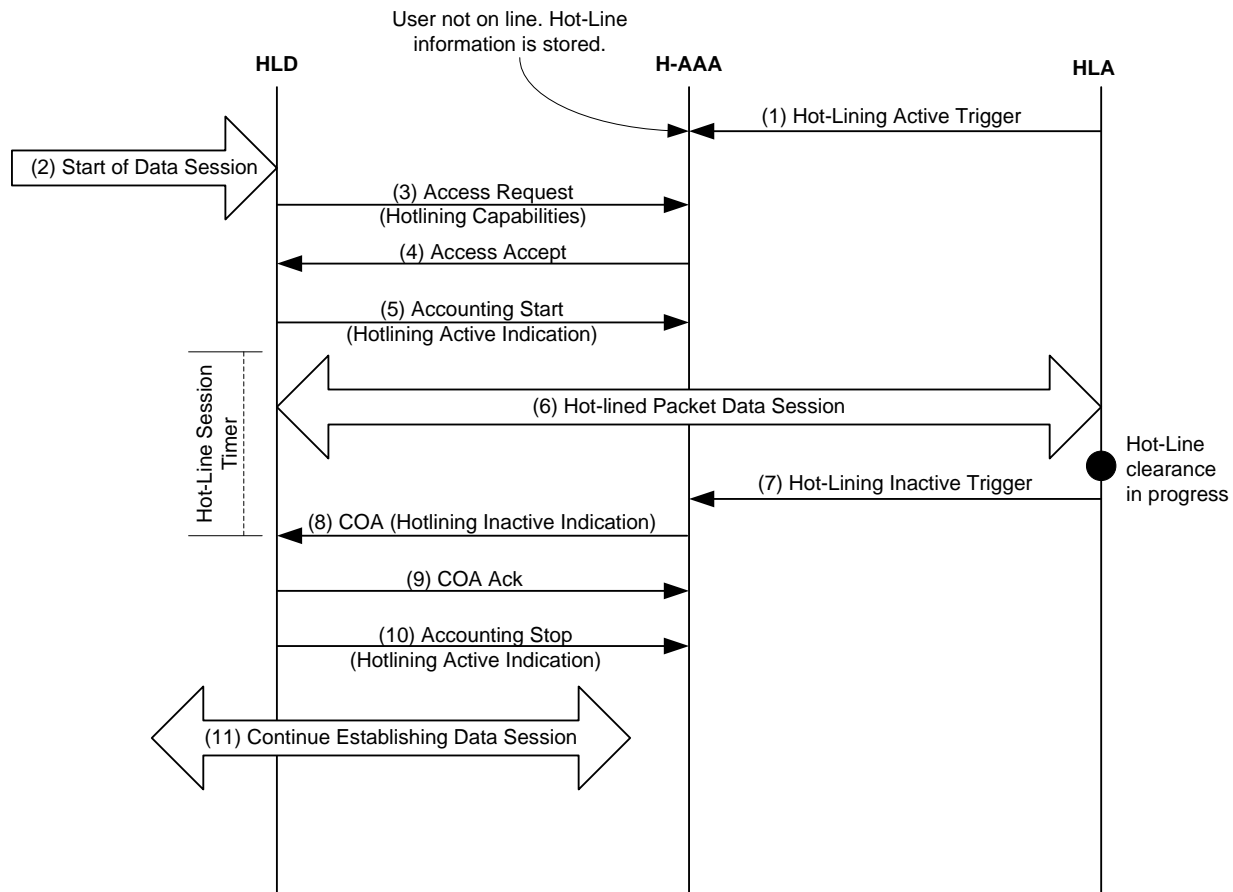


Figure 4-36 – New IP Session Hot-lining

## STEP 1

The HLA hot-lines the user and indicates that to the HAAA by “Hot-lining Active Trigger”. Hot-lining takes in effect when the user attempts to initiate a packet data session (The details of events that cause the HLA to send the Hot-Line Active trigger to the HAAA are not within the scope of this document).

## STEP 2

User attempts to initiate an IP session. This is detected in the ASN as activation of one or more service flow(s).

## STEP 3

Upon detection of new service flow(s) for the user, the HLD sends a RADIUS Access-Request to the HAAA to authorize the user to establish the service flow(s). The HLD includes its Hot-Line capability VSA in the Access-Request.

**STEP 4**

At the HAAA, the local Policy and received Hot-Line Capability in the RADIUS Access-Request is used to determine which HLD will be used to hot-line the session. This is because more than one HLD may send this session setup indication with Hot-Line capability to the HAAA. In case of the HA acting as the HLD, the trigger for detecting a new IP session is the reception of an Mobile IP RRQ or BU from the user. Depending on the type of method (either profile based hot-ling or Rule based Hot-lining) selected at the HAAA, it sends a RADIUS Access-Accept to the HLD with the appropriate attributes.

**STEP 5**

The HLD sends RADIUS Accounting Request (Start) for the hot-lined session. If Session-Timeout attribute was included in step 3, the HLD initiates session teardown (i.e., tear down of the service flows associated with the IP session) when the duration specified in the Session-Timeout attribute has elapsed and the user's session is still hot-lined. After tearing down the service flow(s), the HLD sends an Accounting Request (Stop) to the HAAA to inform that the user's IP session has ended.

**STEP 6**

Based on the Hot-lining rules set at the HAAA and indicated by it in the RADIUS Access-Accept earlier, the uplink and/or downlink data traffic of the user is either dropped/disconnected, or blocked, or blocked and redirected to the HLA by the HLD.

**STEP 7**

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 clear the Hot-line status. The method of notification to the user is undefined in this document.

- If the condition that triggered Hot-lining session does not get cleared, the HLA may terminate the session. In this case, the HAAA is notified by the HLA. Upon receipt of this notification, the HAAA SHALL send a RADIUS Disconnect Message to the HLD where the accounting records are stopped and the session termination is initiated. This may also happen automatically at the HLD, if the user's Hot-Lined status does not change within the duration of the Session-Timeout value.
- Otherwise, if the condition that triggered Hot-lining session gets cleared (via an undefined procedure), the HLA detects this and indicates to the HAAA to clear the Hot-line status of the user by sending the Hot-lining Inactive Trigger to the HAAA.

**STEP 8**

Upon receipt of the Hot-lining Inactive Trigger, the HAAA sends a RADIUS COA message to the HLD with appropriate attributes. Note that this may not be the same HLD that initially handled the activation of the Hot-lining.

**STEP 9**

Upon receipt of the RADIUS COA,

- If the HLD can honor the request then it will respond with a RADIUS COA Ack to the HAAA and Hot-line Session-Timeout timer is turned off.
- If the HLD cannot honor the request then it SHALL respond with a COA NAK message. Based on the local policy, the HAAA may either retry sending the Hot-Lining signal to the HLD or it may send a RADIUS Disconnect Message to the HLD for terminating the IP session.

**STEP 10**

The HLD sends a RADIUS Accounting Request (Stop) to the HAAA.

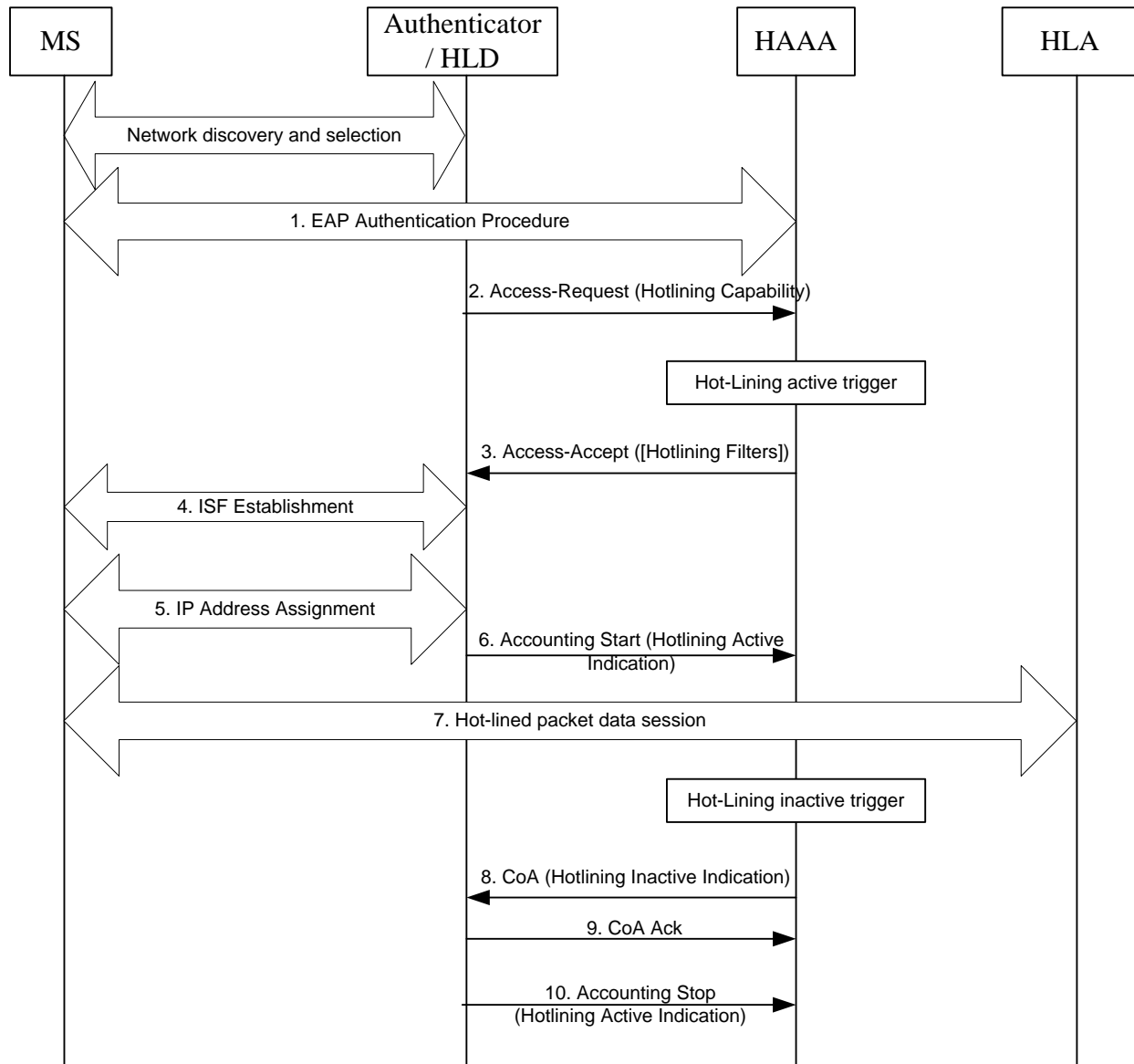
**STEP 11**

User continues establishing the IP session.

#### 4.4.3.5.3 Hot-lining during initial network entry

During initial network entry, Hot-lining MAY be invoked. Triggers for invoking hot-lining are out-of-scope of this section. Examples include limited access to emergency services, empty prepaid accounts, or mobility restriction applying to a fixed or nomadic subscription when H-AAA detects that initial network entry is being performed at a BS that does not belong to the network entry zone of the MS.

Figure 4-37 depicts the call flows between the HLD, HAAA and HLA.



**Figure 4-37 – Hot-lining during initial network entry**

#### STEP 1

The MS performs EAP authentication of initial network entry.

#### STEP 2

The Authenticator sends Access-Request as part of the authentication procedure and the H-AAA server acquires the ASN hot-lining capabilities.



**STEP 3**

If H-AAA decides to activate Hot-lining, it sends an Access-Accept to the Authenticator/HLD with the appropriate attributes, as per section 4.4.3.5.2.

Note: The trigger condition for Hot-lining is out the scope of this section. The H-AAA may determine to activate Hot-lining depending on application specific conditions, such as emergency network entry indicated by ES specific NAI, mobility restrictions applying to fixed or nomadic subscribers, or an empty prepaid account.

**STEP 4**

Anchor SFA located with Authenticator establishes the initial service flow (ISF) for the MS.

**STEP 5**

The MS gets an IP address from network side if IP address is required for Hot-lining.

**STEP 6**

The Authenticator/HLD sends RADIUS Accounting Request (Start) for the hot-lined session to indicate the activation of hot-lining, as per section 4.4.3.5.2.

**STEP 7**

Based on the Hot-Lining rules received from the H-AAA server the uplink and/or downlink data traffic of the user is either dropped/disconnected, or blocked, and redirected to the HLA by the HLD.

**STEP 8**

If the HAAA detects that the condition that triggered the hot-lining of the session gets cleared, the HAAA sends a Radius COA message to the Authenticator/HLD with appropriate attributes.

Note: The trigger condition for the hot-lining inactive indication is out the scope of this section.

**STEP 9**

Upon receipt of the Radius COA, the Authenticator/HLD responds with a Radius COA Ack to the HAAA.

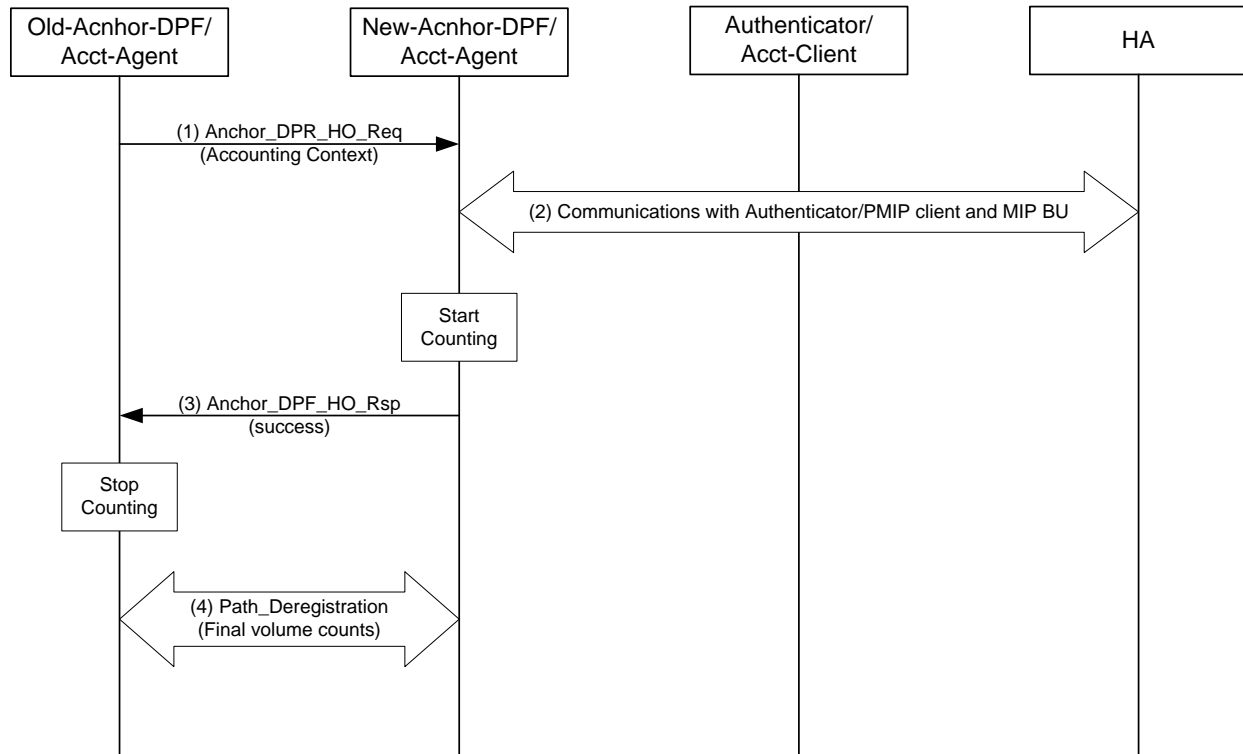
**STEP 10**

The Authenticator/HLD sends a Radius Accounting Request (Stop) to the HAAA to indicate the inactivation of the Hot-lining.

**4.4.3.5.4 Accounting Agent Relocation**

Accounting Agent is collocated with MS' Anchor DPF/ FA functional entities. When Anchor DPF/ FA relocation scenario occurs, the Accounting Agent is also relocated. The PMIP4 scenario is presented in the section [4.8.2.3.7]. The CMIP4 scenario is described in [4.8.3.3].

The below figure refers a generic Anchor DPF relocation scenario highlighting specifics relevant for Accounting Agent relocation.



**Figure 4-38 – Accounting Agent Relocation**

### STEP 1

Anchor DP HO trigger occurs in the “old” Anchor DP entity. This may be a local trigger or instigated by *Anchor\_DPF\_HO\_Trigger* message from the “new” Anchor DP.

The “old” Anchor DP entity initiates Anchor DPF relocation by sending *Anchor\_DPF\_HO\_Req* message to the “new” Anchor DP.

The “old” Accounting Agent should include Accounting Context TLV in this message. The Accounting Context provides the “new” Accounting Agent with the provisioning information for this subscriber. It also contains the remaining duration left in the interim update interval. This is done so the Interim UDRs maintain the consistent interim update interval to the AAA.

### STEP 2

This is a complex step including multiple interactions specific for different scenarios (PMIP4, CMIP4, etc.). As a part of this step, MIP binding update occurs and the “new” Anchor DP updates Authenticator with its location/identity.

For the PMIP4 case this step is represented by steps (3) – (7) on the [4.8.2.3.7].

In the CMIP case, when CSN-anchored HO is successfully completed, the “new” Anchor DP sends *Context\_Rpt* message to Authenticator including Anchor GW Identity TLV. Authenticator receiving this *Context\_Rpt* message updates its notion of the location of Anchor DP entity and confirms it by sending *Context-Ack* message.

### STEP 3

The “new” Anchor DP sends *Anchor\_DPF\_HO\_Rsp* message to the “old” Anchor DP to indicate successful FA relocation. The “new” Anchor DP starts volume counting and the “old” Anchor DP stops volume counting. This helps minimize “double counting”.

#### STEP 4

As part of the R4 Path Deregistration procedure the final volume counts are transferred from the old to the new Accounting Agent. When the new Accounting Agent reports volume counts to the Accounting Client it will include the total cumulative counts (from new and all old Accounting Agents).

##### 4.4.3.5.5 Context update procedure for Hot-Lining

When the Accounting Agent (always co-located with the Anchor DPF) and Accounting Client (always co-located with the Anchor Authenticator) are not co-located, R4 messaging between the two entities for Hot-Lining is necessary.

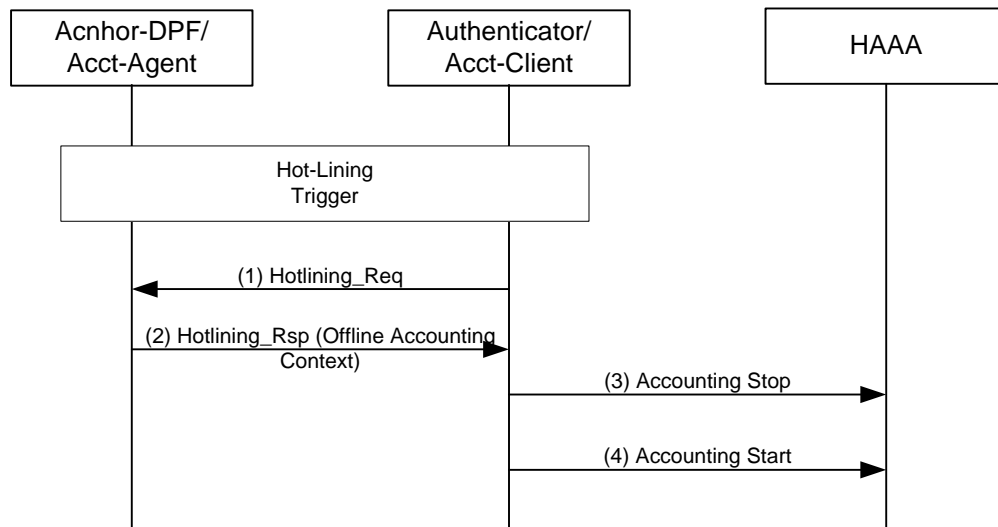


Figure 4-39 – Context Update procedure

#### STEP 1

When a subscriber is hotlined or un-hotlined, the Accounting Client needs to know the volume counts at that transition. In this case it requests those volume counts from the Accounting Agent over R4 using the Hotlining\_Req message with the Offline Accounting Context bit set.

#### STEP 2

The Accounting Agent receives the Hotlining-Req message and responds with a Hotlining\_Rsp message which contains the Offline Accounting Context TLV.

#### STEP 3

The Accounting Client sends Accounting Stop (with Session-Continue set to True and Hotlining-Indication set appropriately) to the HAAA to capture the volume counts at the Hot-Lining transition.

#### STEP 4

The Accounting Client also sends Accounting Start (with Beginning-of-Session set to False and Hotlining-Indication set appropriately) to the HAAA at the Hot-Lining transition.

#### 4.4.3.6 Accounting Messages

##### 4.4.3.6.1 R6 Reference Point

##### 4.4.3.6.1.1 RR\_Req (Create) / HO\_Req / Context\_Rpt / IM\_Exit\_State\_Change\_Rsp

The Accounting Extensions TLV is sent in *RR\_Req* (Create) during Service Flow Creation, in *HO\_Req* during Controlled HO, in *Context\_Rpt* during Uncontrolled HO and *IM\_Exit\_State\_Change\_Rsp* during Idle Mode Exit. The TLV is included only once even if multiple flows are included in the message.

**Table 4-32 – RR\_Req (Create) / HO\_Req / Anchor\_DPF\_HO\_Req (for R4 only) / Context\_Rpt / IM\_Exit\_State\_Change\_Rsp Message Structure**

IE	Description	M/O	Notes
...			<p>For a complete list of the additional IEs in the <i>RR_Req</i> message, see Table 4-59 and Table 4-60 for R4.</p> <p>For a complete list of the additional IEs in the <i>HO_Req</i> message, see Table 4-82.</p> <p>For a complete list of the additional IEs in the <i>Anchor_DPF_HO_Req</i> message, see Table 4-113 and Table 4-133. <i>Anchor_DPF_HO_Req</i> applies to R4 only.</p> <p>For a complete list of the additional IEs in the <i>Context_Rpt</i> message, see Table 4-20, Table 4-84, Table 4-93, Table 4-156 and Table 4-178 for R4.</p> <p>For a complete list of the additional IEs in the <i>IM_Exit_State_Change_Rsp</i> message, see Table 4-174 for R4 and Table 4-171 for R6.</p>
Accounting Context	5.3.2.204	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.
>Accounting Mode Provisioning	5.3.2.243	CM	This TLV SHALL be included if Accounting Context is included in the transmitted message.
>>Accounting Type	5.3.2.247	CM	This TLV SHALL be included if Accounting Mode Provisioning is included in the transmitted message.
>> Interim Update Interval	5.3.2.248	O	The Interim Update Interval is data field in the AAA server and sent to the Accounting Client in the <i>Access_Accept</i> message. This TLV is only used for volume-based accounting. This TLV SHALL be included in <i>Anchor_DPF_HO_Req</i> messages. <i>Anchor_DPF_HO_Req</i> applies to R4 only.
>>Accounting Number of ToDs	5.3.2.256	O	The number of Time of Day Tariff Switch TLVs.
>>Time of Day Tariff Switch	5.3.2.253	O	The Time of Day Tariff Switch TLV is data field in the AAA server and sent to the ASN-GW in the <i>Access-Accept</i> packet. There can be more than one of these sent.

IE	Description	M/O	Notes
>>>Time of Day Tariff Switch Time	5.3.2.254	CM	The time of day time in hours and minutes. This TLV SHALL be included if Time of Day Tariff Switch is included in the transmitted message.
>>>Time of Day Tariff Switch Offset	5.3.2.255	CM	The time of day timezone offset This TLV SHALL be included if Time of Day Tariff Switch is included in the transmitted message.
>Interim Update Interval Remaining	5.3.2.287	O	This TLV SHALL be included in Anchor_DPF_HO_Req messages. Anchor_DPF_HO_Req applies to R4 only.

#### 4.4.3.6.1.2 RR\_Rsp (Modify and Delete)

*RR\_Rsp* (Modify and Delete) contains the Accounting Session/Flow Volume Counts TLV for Service Flow Modification and Deletion. If per service flow accounting information is reported by the accounting agent, accounting information associated with one or more service flows are included in the *RR\_Rsp* (Modify and Delete) then a separate Accounting Session/Flow Volume Counts TLV should be included for each flow.

**Table 4-33 – RR\_Rsp (Modify and Delete) Message Structure**

IE	Description	M/O	Notes
...			For a complete list of the additional IEs in the <i>RR_Rsp</i> message, see Table 4-57 and Table 4-58 for R4.
Offline Accounting Context	5.3.2.360	O	
>Accounting Bulk Session/Flow Volume Counts	5.3.2.359	CM	This TLV SHALL be included if Offline Accounting Context is included in the transmitted message.
>>Accounting Number of Bulk Sessions	5.3.2.245	CM	This TLV SHALL be included if Accounting Bulk Session/Flow Volume Counts is included in the transmitted message.
>>Accounting Bulk Session/Flow	5.3.2.246	CM	This TLV SHALL be included if Accounting Bulk Session/Flow Volume Counts is included in the transmitted message.
>>>SFID	5.3.2.184	O	
>>>Accounting IP Address	5.3.2.264	CM	This TLV SHALL be included if Accounting Bulk Session/Flow is included in the transmitted message.
>>>Accounting Session/Flow Volume Counts	5.3.2.244	CM	This TLV SHALL be included if Accounting Bulk Session/Flow is included in the transmitted message.
>>>>Cumulative Uplink Octets	5.3.2.249	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.

IE	Description	M/O	Notes
>>>>Cumulative Downlink Octets	5.3.2.250	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Cumulative Uplink Packets	5.3.2.251	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Cumulative Downlink Packets	5.3.2.252	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Uplink Octets at Tariff Switch	5.3.2.257	O	
>>>>Downlink Octets at Tariff Switch	5.3.2.258	O	
>>>>Uplink Packets at Tariff Switch	5.3.2.259	O	
>>>>Downlink Packets at Tariff Switch	5.3.2.260	O	

#### 4.4.3.6.1.3 Bulk Interim Update

The Bulk Interim Update contains volume counts for several subscribers in one message. It is only used for volume-based accounting. This message is sent by the serving BS to the serving ASN-GW. The Ack message does not contain any TLVs, it is just a confirmation to the BS that the ASN-GW received the Bulk Interim Update. Volume counts from different subscribers may be gathered in a single Bulk Interim Update message if their corresponding "Interim Update Interval"s expire at the same time at the Accounting Agent side. The accounting client at the ASN-GW will then unbundle the bulk counts and construct the UDRs separately for each MS based on the corresponding MSID and the accounting granularity.

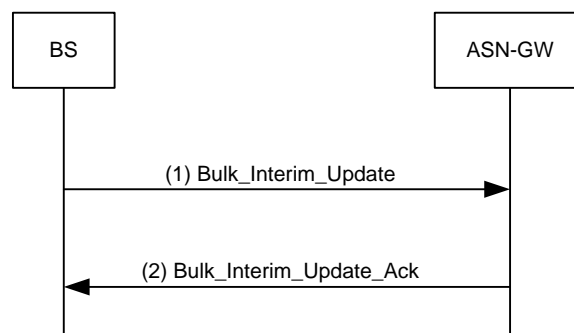


Figure 4-40 – Bulk Interim Update

Table 4-34 – Bulk Interim Update Message Structure

IE	Description	M/O	Notes
Offline Accounting Context	5.3.2.360	M	
>Accounting Bulk Session/Flow Volume Counts	5.3.2.359	M	

IE	Description	M/O	Notes
>>Accounting Number of Bulk Sessions	5.3.2.245	M	
>>Accounting Bulk Session/Flow	5.3.2.246	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.
>>>MSID	5.3.2.102	O	
>>>SFID	5.3.2.184	O	
>>>Accounting IP Address	5.3.2.264	M	
>>>Accounting Session/Flow Volume Counts	5.3.2.244	M	
>>>>Cumulative Uplink Octets	5.3.2.249	M	
>>>>Cumulative Downlink Octets	5.3.2.250	M	
>>>>Cumulative Uplink Packets	5.3.2.251	M	
>>>>Cumulative Downlink Packets	5.3.2.252	M	
>>>>Uplink Octets at Tariff Switch	5.3.2.257	O	
>>>>Downlink Octets at Tariff Switch	5.3.2.258	O	
>>>>Uplink Packets at Tariff Switch	5.3.2.259	O	
>>>>Downlink Packets at Tariff Switch	5.3.2.260	O	

#### 4.4.3.6.1.4 Path Dereg Req / IM\_Entry\_State\_Change\_Req / NetExit\_MS\_State\_Change\_Req/Rsp

R6 *Path\_Dereg\_Req* and R6 *IM\_Entry\_State\_Change\_Req* and R6 *NetExit\_MS\_State\_Change\_Req/Rsp* messages contain the Accounting Bulk Session/Flow Volume Counts Info TLV for Idle Mode Entry MS de-registration from the network and MS Network Exit procedures. The *Path\_Dereg\_Req/IM\_Entry\_State\_Change\_Req / NetExit\_MS\_State\_Change\_Req/Rsp* message structure is described in Table 4-35.

#### 4.4.3.6.2 R4 Reference Point

##### 4.4.3.6.2.1 RR\_Req (Create) / HO\_Req / Anchor\_DPF\_HO\_Req / Context\_Rpt / IM\_Exit\_State\_Change\_Rsp

The Accounting Extensions TLV is sent in the *RR\_Req* (Create) during Service Flow Creation, in *HO\_Req* during Controlled HO, and in *Context\_Rpt* and *IM\_Exit\_State\_Change\_Rsp* during Idle Mode Exit. The TLV is included only once even if multiple flows are included in the message. The *RR\_Req* (Create)/*HO\_Req*/*Anchor\_DPF\_HO\_Req / Context\_Rpt / IM\_Exit\_State\_Change\_Rsp* message structure is described in Table 4-29.

#### 4.4.3.6.2.2 RR\_Rsp (Modify and Delete)

The *RR\_Rsp* (Modify and Delete) contains the Accounting Session/Flow Volume Counts TLV for Service Flow Modification and Deletion. If the ASN receives the Accounting Session/Service Flow Volume Counts TLV in the *RR\_Rsp*, this TLV is relayed in the *RR\_Rsp* message to the ASN where the Accounting Client is resided. If per service flow accounting information is reported by the accounting agent, separate Accounting Session/Flow Volume Counts TLV should be included for each flow. The *RR\_Rsp* (Modify and Delete) message structure is described in Table 4-30.

#### 4.4.3.6.2.3 Bulk Interim Update

The *Bulk Interim Update* message contains volume counts for several subscribers in one message. It is only used for volume-based accounting. When the accounting client is located in a different ASN-GW, this message is sent by the serving GW over the R4 interface upon receipt of a similar Bulk Interim Update message from the serving BS over the R6 interface. Note that the response message does not contain any TLVs. The *Bulk\_Interim\_Update* message is described in table 4-31.

#### 4.4.3.6.2.4 Path\_Dereg\_Req / IM\_Entry\_State\_Change\_Req / NetExit\_MS\_State\_Change\_Req/Rsp

R4 *Path\_Dereg\_Req* and R4 *IM\_Entry\_State\_Change\_Req* and R4 *NetExit\_MS\_State\_Change\_Req/Rsp* messages contain the Accounting Bulk Session/Flow Volume Counts TLV for Idle Mode Entry MS de-registration from the network and MS Network Exit procedures.

**Table 4-35 – Path\_Dereg\_Req / IM\_Entry\_State\_Change\_Req /  
NetExit\_MS\_State\_Change\_Req/Rsp Message Structure**

IE	Description	M/O	Notes
...			For a complete list of the additional IEs in the Path_Dereg_Req message, see Table 4-44 for R4, and Table 4-62 and Table 7-21 for R6. For a complete list of the additional IEs in the IM_Entry_State_Change_Req message, see Table 4-149 for R4 and Table 4-146 for R6. For a complete list of the additional IEs in the NetExit_MS_State_Change_Req message, see Table 4-45 for R4/R6. For a complete list of the additional IEs in the NetExit_MS_State_Change_Rsp message, see Table 4-46 for R4/R6.
MS Info	5.3.2.103	O	This TLV SHALL be present in the NetExit_MS_State_Change_Req/Rsp to update used Quota in case of Prepaid user during Network Exit Procedure.
>PPAQ	5.3.2.131	O	Used for quota request.
>>Quota Identifier	5.3.2.148	CM	This TLV SHALL be included if PPAQ is included in the transmitted message.
>>Volume Quota	5.3.2.167	O	
>>Volume Threshold	5.3.2.168	O	
>>Volume Used	5.3.2.168	O	
>>Duration Quota	5.3.2.275	O	



IE	Description	M/O	Notes
>>Duration Threshold	5.3.2.276	O	
>> Duration used	5.3.2.132	O	
>>Resource Quota	5.3.2.277	O	
>>Resource Threshold	5.3.2.278	O	
>>Update Reason	5.3.2.279	O	
>>Service-ID	5.3.2.280	O	
>>Rating-Group-ID	5.3.2.281	O	
>>Termination Action	5.3.2.282	O	
>>Pool-ID	5.3.2.283	O	
>>Pool-Multiplier	5.3.2.284	O	
>>Prepaid Server	5.3.2.285	O	This TLV SHOULD be included if available (provided by HAAA)
>>SFID (one or more)	5.3.2.184	O	SF ID(s) SHALL be included in flow based prepaid accounting scenario.
Offline Accounting Context	5.3.2.360	O	
Accounting Bulk Session/Flow Volume Counts	5.3.2.359	CM	This TLV SHALL be included if Offline Accounting Context is included in the transmitted message.  This accounting extension is exchanged between ASNs for Idle Mode Entry MS de-registration from the network and MS Network Exit.
>>Accounting Number of Bulk Sessions	5.3.2.245	CM	This TLV SHALL be included if Accounting Bulk Session/Flow Volume Counts is included in the transmitted message.
>>Accounting Bulk Session/Flow	5.3.2.246	CM	This TLV SHALL be included if Accounting Bulk Session/Flow Volume Counts is included in the transmitted message.
>>>SFID	5.3.2.184	O	
>>>Accounting IP Address	5.3.2.264	CM	This TLV SHALL be included if Accounting Bulk Session/Flow is included in the transmitted message.
>>>Accounting Session/Flow Volume Counts	5.3.2.244	CM	This TLV SHALL be included if Accounting Bulk Session/Flow is included in the transmitted message.
>>>>Cumulative Uplink Octets	5.3.2.249	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Cumulative Downlink Octets	5.3.2.250	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.

IE	Description	M/O	Notes
>>>>Cumulative Uplink Packets	5.3.2.251	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Cumulative Downlink Packets	5.3.2.252	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Uplink Octets at Tariff Switch	5.3.2.257	O	
>>>>Downlink Octets at Tariff Switch	5.3.2.258	O	
>>>>Uplink Packets at Tariff Switch	5.3.2.259	O	
>>>>Downlink Packets at Tariff Switch	5.3.2.260	O	

1

#### 2 4.4.3.6.2.5 Prepaid\_Request / Prepaid\_Notify Messages

3 These messages are used over R4 for online accounting events communication between PPA and PPC (quota  
4 requests and quota updates). *Prepaid Request* message SHALL include PPAQ (quota) TLV. *Prepaid Notify* message  
5 SHALL include PPAQ (quota) TLV if quota update is performed. In the case there is no additional resources for the  
6 particular service, PPC sends *Prepaid Notify* message to PPA without PPAQ.

7

**Table 4-36 – Prepaid\_Request Message Structure**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>PPAQ	5.3.2.131	M	Used for quota request.
>>Quota Identifier	5.3.2.148	M	
>>Volume Quota	5.3.2.167	O	
>>Volume Threshold	5.3.2.168	O	
>>Volume Used	5.3.2.357	O	
>>Duration Quota	5.3.2.275	O	
>>Duration Threshold	5.3.2.276	O	
>>Resource Quota	5.3.2.277	O	
>>Resource Threshold	5.3.2.278	O	
>>Update Reason	5.3.2.279	O	
>>Service-ID	5.3.2.280	O	
>>Rating-Group-ID	5.3.2.281	O	
>>Termination Action	5.3.2.282	O	
>>Pool-ID	5.3.2.283	O	

IE	Reference	M/O	Notes
>>Pool-Multiplier	5.3.2.284	O	
>>Prepaid Server	5.3.2.285	O	This TLV SHOULD be included if available (provided by HAAA).
>>SFID (one or more)	5.3.2.184	O	SF ID(s) SHALL be included in flow based prepaid accounting scenario.

**Table 4-37 – Prepaid\_Notify Message Structure**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	O	
>PPAQ	5.3.2.131	O	Used for quota request.
>>Quota Identifier	5.3.2.148	CM	This TLV SHALL be included if PPAQ is included in the transmitted message.
>>Volume Quota	5.3.2.167	O	
>>Volume Threshold	5.3.2.168	O	
>>Volume Used	5.3.2.357	O	
>>Duration Quota	5.3.2.275	O	
>>Duration Threshold	5.3.2.276	O	
>>Resource Quota	5.3.2.277	O	
>>Resource Threshold	5.3.2.278	O	
>>Update Reason	5.3.2.279	O	
>>Service-ID	5.3.2.280	O	
>>Rating-Group-ID	5.3.2.281	O	
>>Termination Action	5.3.2.282	O	
>>Pool-ID	5.3.2.283	O	
>>Pool-Multiplier	5.3.2.284	O	
>>Prepaid Server	5.3.2.285	O	This TLV SHOULD be included if available (provided by HAAA)
>>SFID (one or more)	5.3.2.184	O	SF ID(s) SHALL be included in flow based prepaid accounting scenario.

#### 4.4.3.6.2.5.1 Prepaid Quota Update Procedure Timers and Timer Consideration

This section identifies the timer entities participating in the Prepaid Section. The following timers are defined over R4:

- $T_{\text{Prepaid\_Request}}$ : is started by PPA requesting the Prepaid Quota from PPC, upon sending Prepaid\_Request Message and it is stopped upon receiving a Corresponding Prepaid\_Notify Message from PPC.

Table 4-38 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-38 – Timer Values for Prepaid Messages over R4**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
T <sub>Prepaid_Request</sub>	TBD		TBD

#### 4.4.3.6.2.5.2 Prepaid Quota Update Procedure Error Conditions

##### 4.4.3.6.2.5.2.1 Timer Expiry

Table 4-39 shows details on the corresponding actions associated with timer expiry. 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 4-39 Timer Expiry Conditions.

**Table 4-39 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T <sub>Prepaid_Request</sub>	PPA	No action required.

#### 4.4.3.6.2.6 Hotlining\_Req/Hotlining\_Rsp Messages

When PPC and HLD are not Collocated; Hotlining Req and Hotlining Rsp Messages are used to transfer the Hot-Lining Information from PPC to HLD over R4.

**Table 4-40 – Hotlining\_Req [PPC to HLD]**

IE	Description	M/O	Notes
Hotlining Context	5.3.2.400	O	TC bit is set to 1.
> R3 IP-Redirection-Rule	5.3.2.403	O	Usage as specified in 5.4.1.4.
> R3 NAS-Filter-Rule	5.3.2.404	O	Usage as specified in 5.4.1.4.
> R3 Hotline-Session-Timer	5.3.2.405	O	Usage as specified in 5.4.1.4.
> R3 Hotline-Indication	5.3.2.407	O	Usage as specified in 5.4.1.4.
> R3 HTTP-Redirection-Rule	5.3.2.402	O	Usage as specified in 5.4.1.4.
> Service-Id	5.3.2.280	O	Used to identify the Hotlining Context on the Expiry of PPAQ with Same Service ID.

1

**Table 4-41 – Hotlining\_Rsp [HLD to PPC]**

IE	Description	M/O	Notes
Failure Indication	5.3.2.69	O	
Hotlining Context	5.3.2.400	O	TC bit is set to 1.
> Service-Id	5.3.2.280	O	
Offline Accounting Context	5.3.2.360	O	
>Accounting Bulk Session/Flow Volume Counts	5.3.2.359	CM	This TLV SHALL be included if the Offline Accounting Context is included in the transmitted message.
>>Accounting Number of Bulk Sessions	5.3.2.245	CM	This TLV SHALL be included if Accounting Bulk Session/Flow Volume Counts is included in the transmitted message.
>>Accounting Bulk Session/Flow	5.3.2.246	CM	This TLV SHALL be included if Accounting Bulk Session/Flow Volume Counts is included in the transmitted message.
>>>SFID	5.3.2.184	O	
>>>Accounting IP Address	5.3.2.264	CM	This TLV SHALL be included if Accounting Bulk Session/Flow is included in the transmitted message.
>>>Accounting Session/Flow Volume Counts	5.3.2.244	CM	This TLV SHALL be included if Accounting Bulk Session/Flow is included in the transmitted message.
>>>>Cumulative Uplink Octets	5.3.2.249	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Cumulative Downlink Octets	5.3.2.250	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Cumulative Uplink Packets	5.3.2.251	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Cumulative Downlink Packets	5.3.2.252	CM	This TLV SHALL be included if Accounting Session/Flow Volume Counts is included in the transmitted message.
>>>>Uplink Octets at Tariff Switch	5.3.2.257	O	
>>>>Downlink Octets at Tariff Switch	5.3.2.258	O	
>>>>Uplink Packets at Tariff Switch	5.3.2.259	O	
>>>>Downlink Packets at Tariff Switch	5.3.2.260	O	

2

#### 4.4.3.7 Accounting Events in the ASN

The accounting events control the generation of Accounting-Request Start, Stop and Interim messages at the Accounting Client in the ASN.

The accounting client collocated in the Authenticator ASN SHALL generate the Accounting-Start or Accounting-Stop messages based on some events as described below and based on the accounting type indicator received from the HAAA in the Access-Accept packet at the time of Authentication.

The Accounting-Request Start message is sent when one of the following events occurs at the Accounting Client:

- a. When an IP address is assigned to the MS.
- b. At a specific time of the day.
- c. At the onset of Hot-Lining of an ongoing IP session.
- d. At the reset of Hot-Lining of an ongoing IP session.
- e. In case of PD flow based accounting, at the time when a PDFID is allocated to a service flow.
- f. Upon successful modification of the QoS properties of a PD flow (subsequent to an Accounting-Request Stop for the QoS modification).

The Accounting-Request Stop message is sent when one of the following events occurs at the Accounting Client:

- a. When an IP address is de-allocated for the MS. This is normally the indication of an IP session termination.
- b. At a specific time of the day.
- c. At the onset of Hot-Lining of an ongoing IP session.
- d. At the reset of Hot-Lining of an ongoing IP session.
- e. In case of PD flow based accounting, at the time when service flow terminated for the PDFID.
- f. Due to overflow of any of the counters.
- g. Upon successful modification of the QoS properties of a PD flow (prior to an Accounting-Request Start for the QoS modification).

#### 4.4.3.8 Accounting Events in the CSN

The accounting client in the Home Agent in the CSN SHALL generate Accounting-Request Start message based on the following events:

- a. Upon successful creation of a mobility binding for an MS.
- b. Upon successful modification of an ongoing mobility binding for an MS (subsequent to an Accounting-Request Stop for the ongoing mobility binding).
- c. At a specific time of the day.
- d. At the onset of Hot-Lining of an ongoing IP session.
- e. At the reset of Hot-Lining of an ongoing IP session.

The accounting client in the Home Agent in the CSN SHALL generate Accounting-Request Stop message based on the following events:

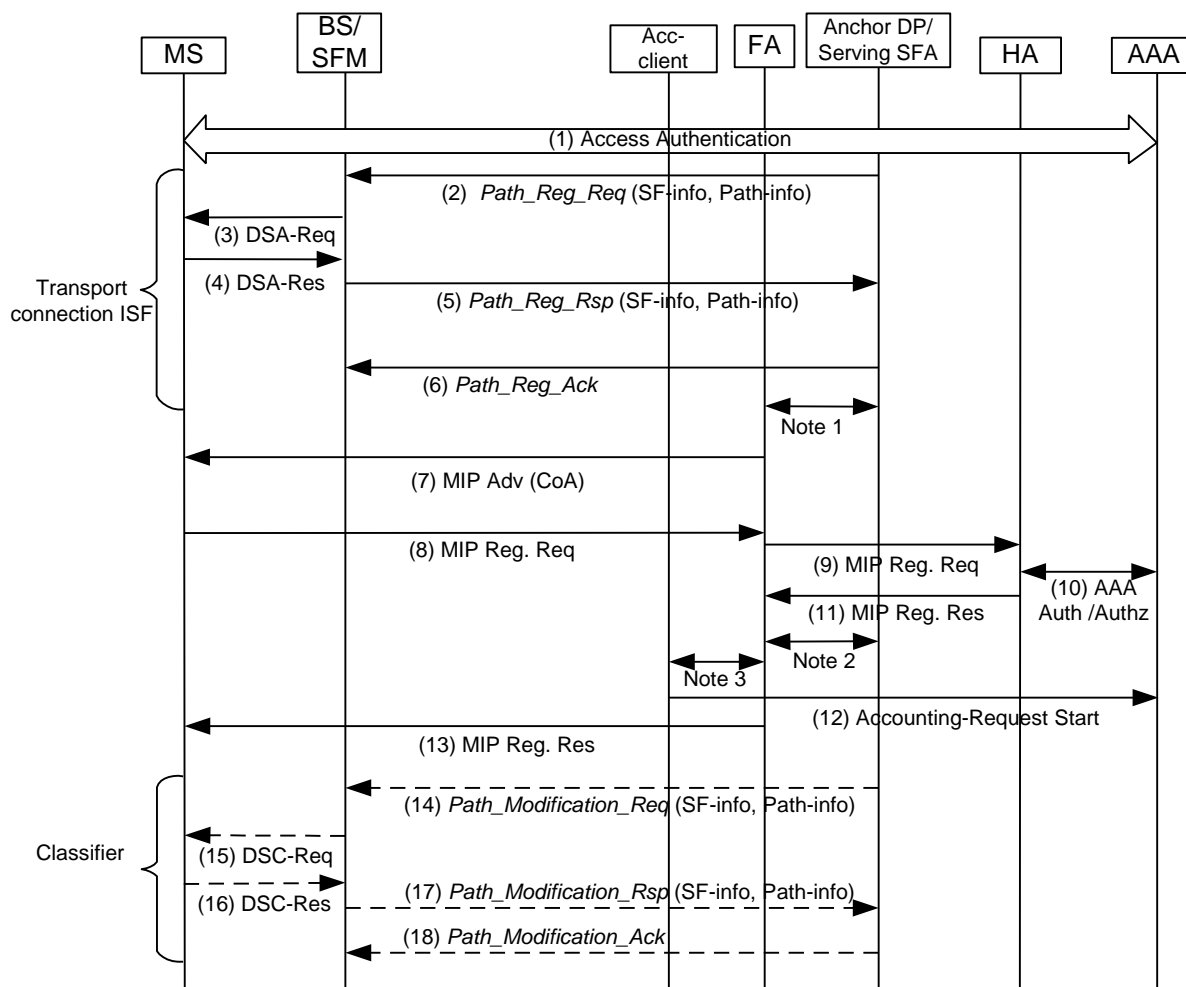
- a. Upon successful deletion of a mobility binding for an MS.
- b. Upon successful modification of an ongoing mobility binding for an MS (prior to an Accounting-Request Start for the ongoing mobility binding).
- c. At a specific time of the day.
- d. At the onset of Hot-Lining of an ongoing IP session.
- e. At the reset of Hot-Lining of an ongoing IP session.

1 f. Due to overflow of any of the counters.

2 **4.4.3.9 Illustrations of the Accounting Start Events in the ASN**

3 The purpose of the figures in this section is to contextualize the accounting triggers. The figures are informative.

4 For further details refer to the specific sections in this document.



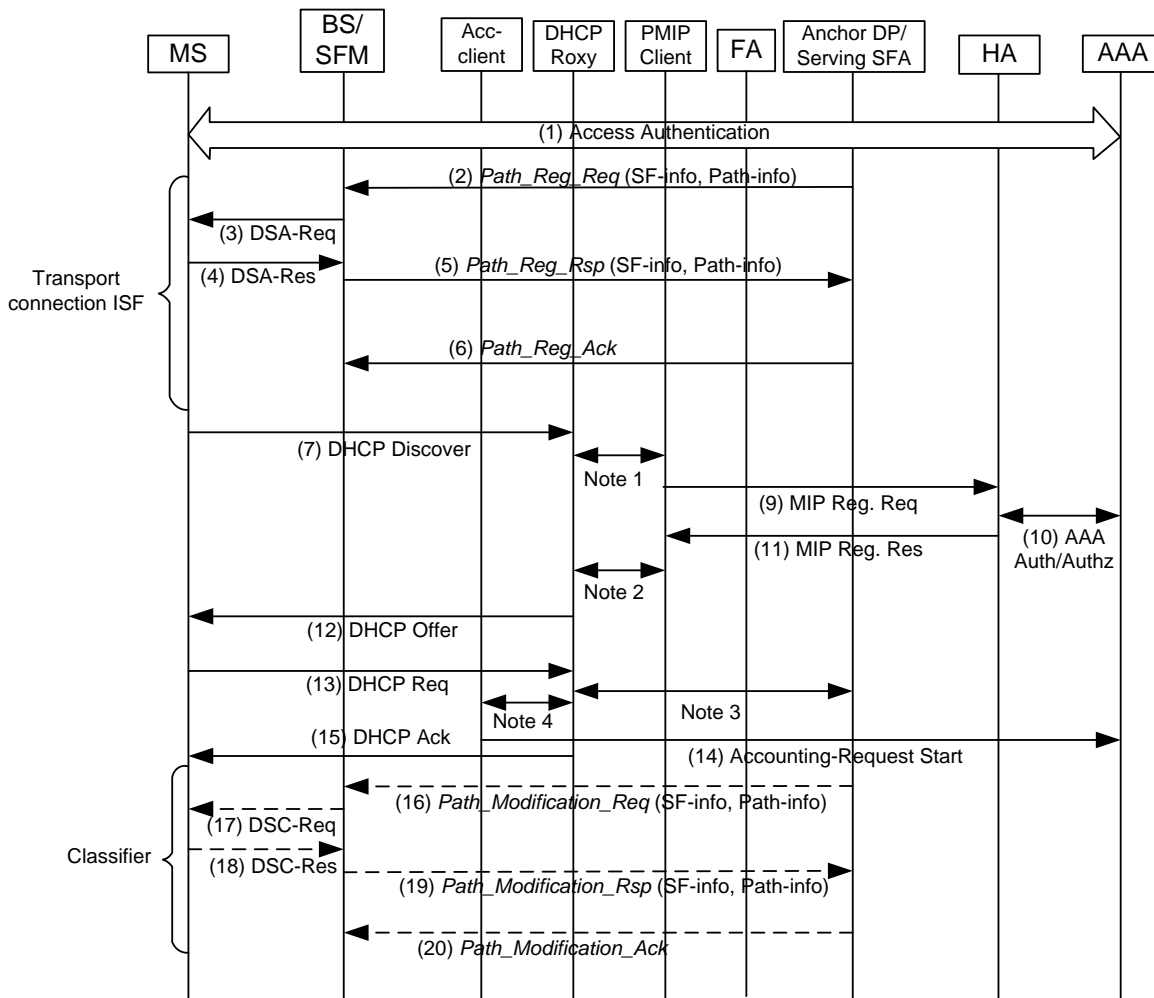
Note 1: Serving SFA triggers FA to initiate MIP registration (out of scope of spec)

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)

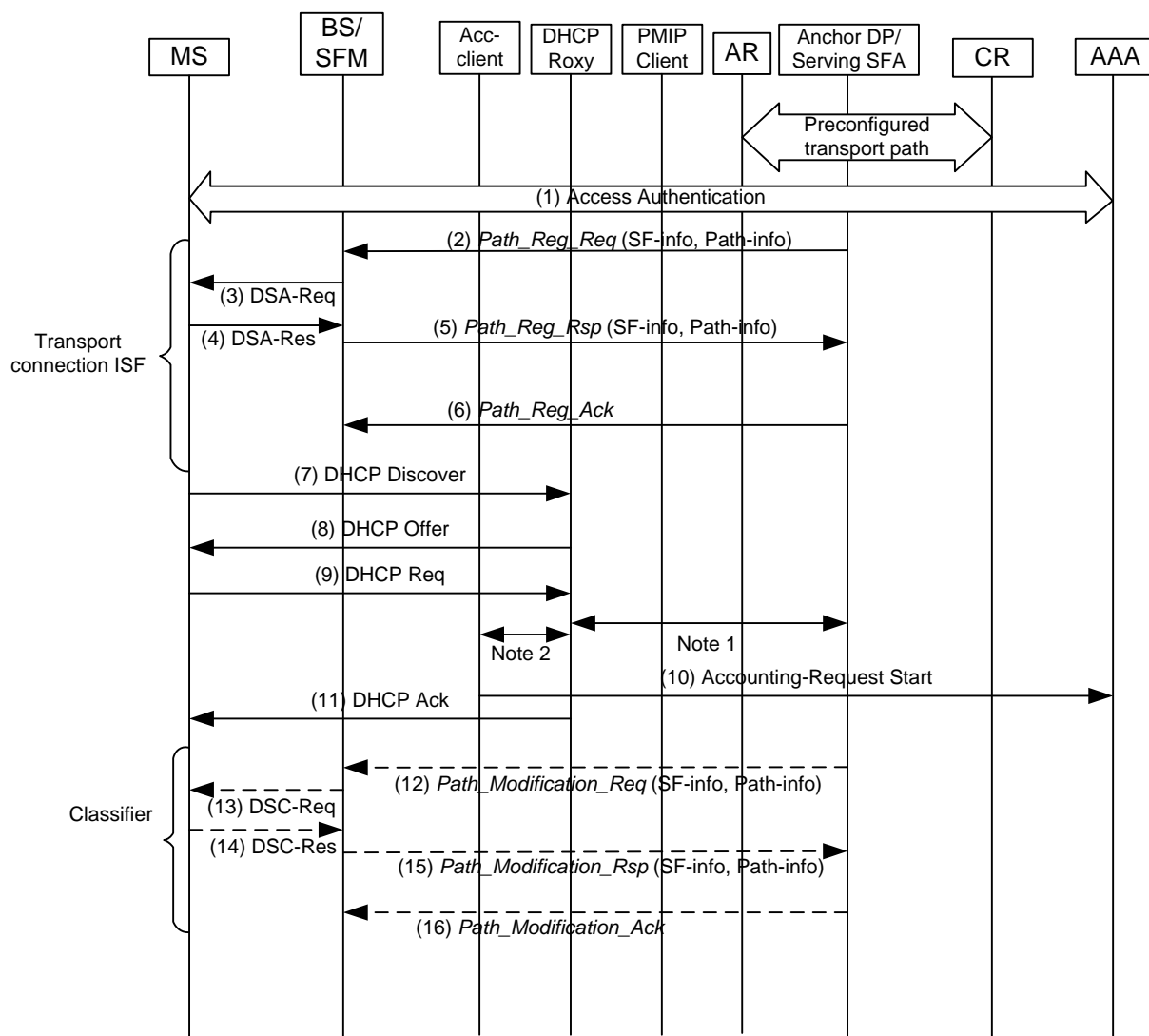
**Figure 4-41 – Accounting Start Event in the ASN in Case of CMIP4**





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)

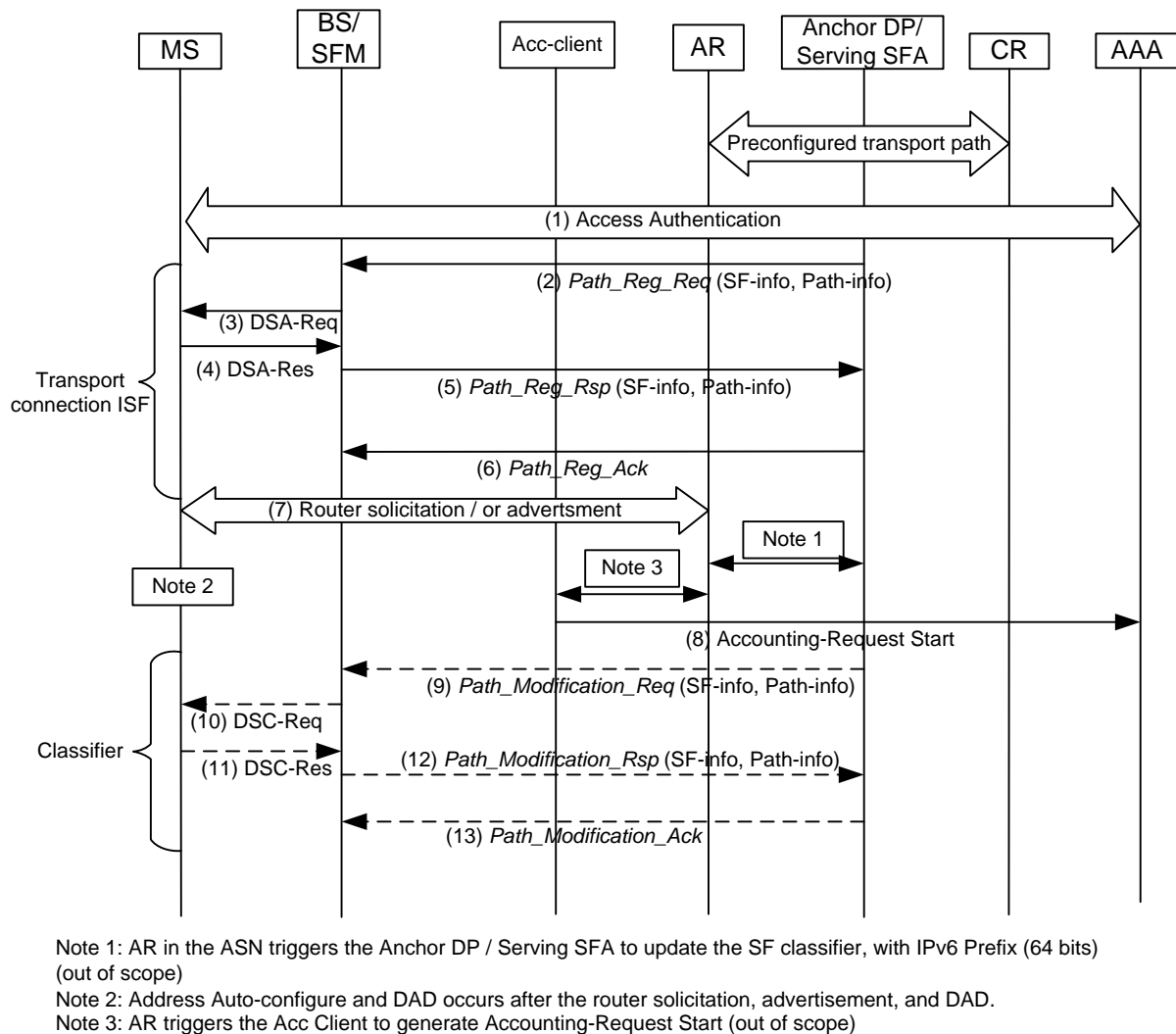
**Figure 4-42 – Accounting Start Event in the ASN in Case of PMIP4**



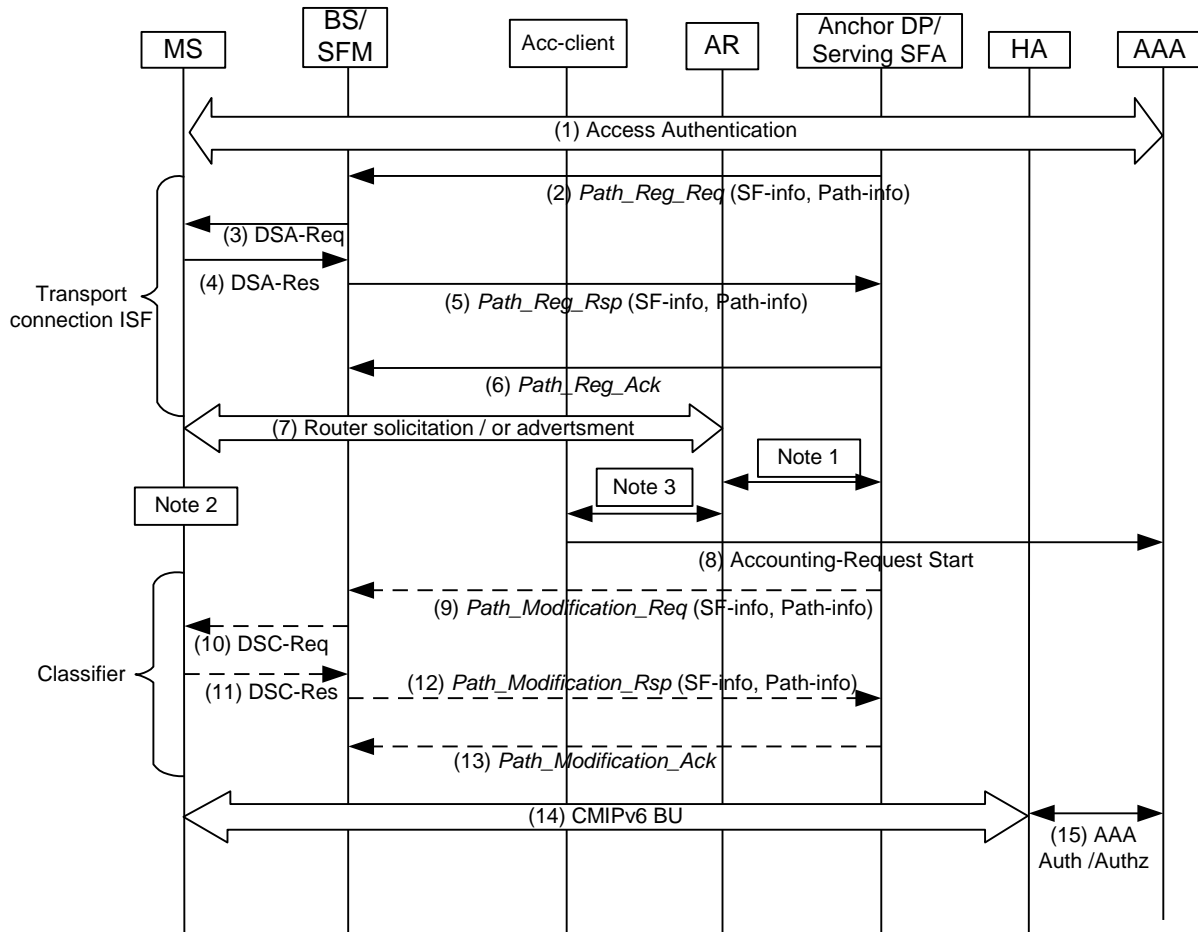
Note 1: DHCP proxy triggers the Anchor DP/Serving SFA to update the SF classifier. (out of scope of this section)

Note 2: DHCP proxy triggers the Acc Client to generate Accounting-Request Start (out of scope of this section)

**Figure 4-43 – Accounting Start Event in the ASN in Case of Simple IPv4**

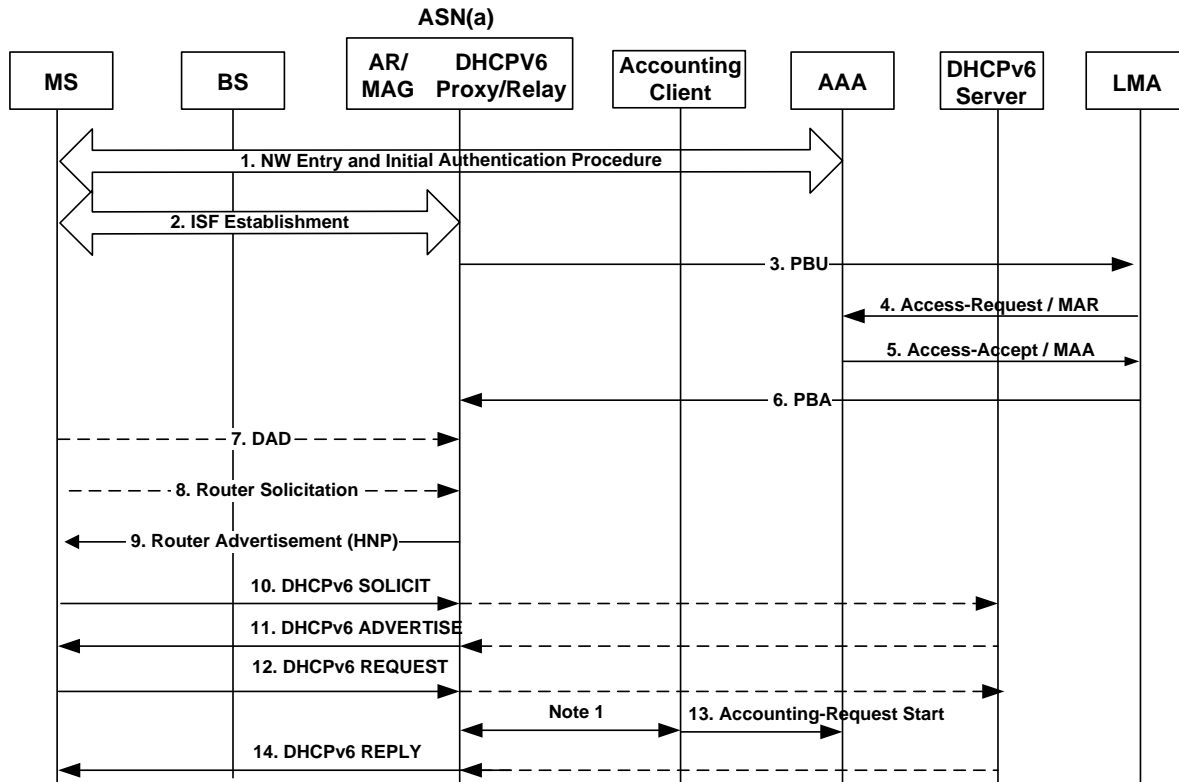


**Figure 4-44 – Accounting Start Event in the ASN in Case of Simple IPv6**



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)

**Figure 4-45 – Accounting Start Event in the ASN in Case of CMIP6 (note CMIP6 has no accounting event in ASN)**



Note 1: ASN(a) triggers Accounting Client to generate Accounting-Request Start message (out of scope)

**Figure 4-46 – Accounting Start Event in the ASN in case of PMIPv6**

#### 4.4.3.10 Illustrations of the Accounting Start Events in the CSN

The purpose of the figures in this section is to contextualize the accounting triggers. The figures are informative. For further details refer to the specific sections in this document.

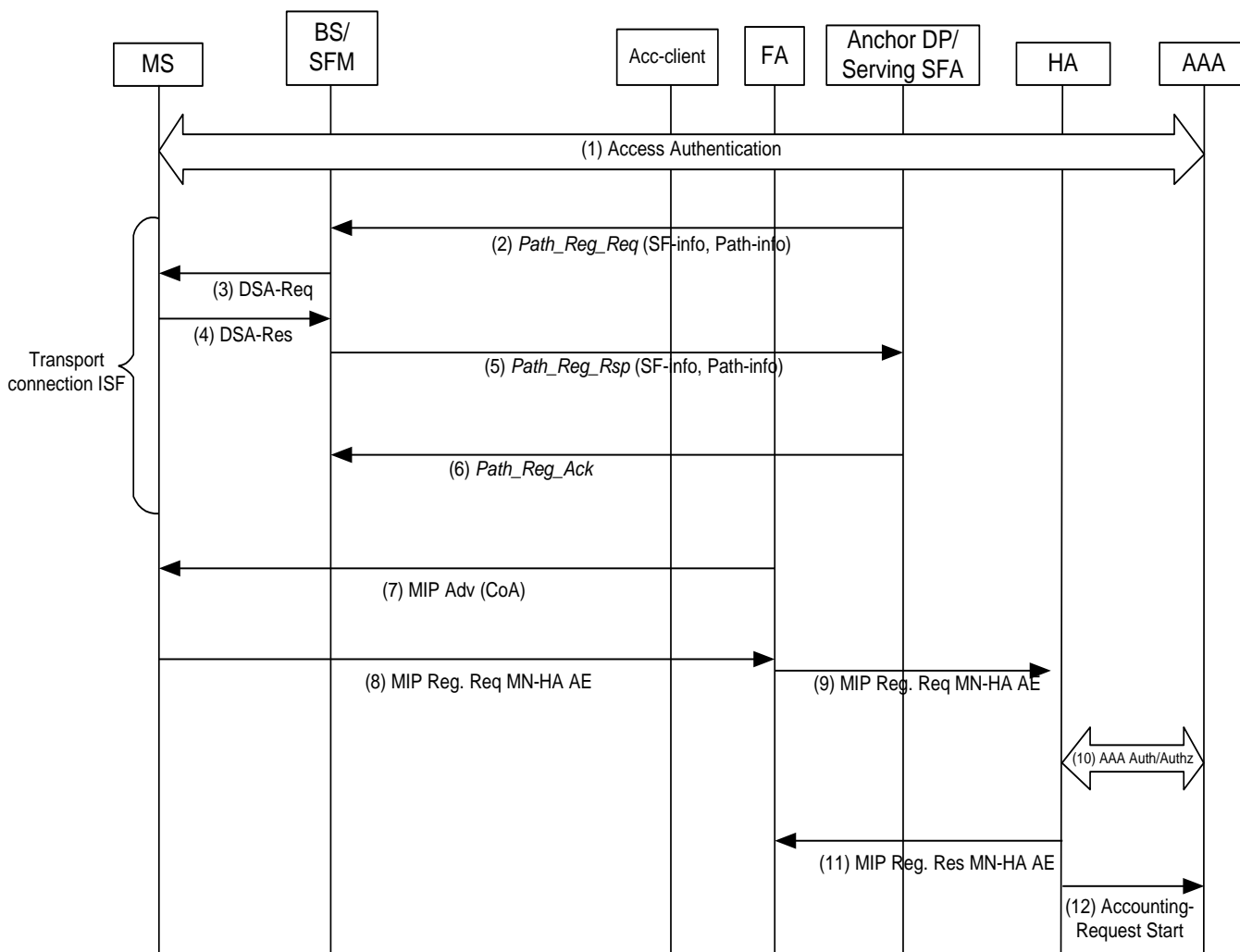
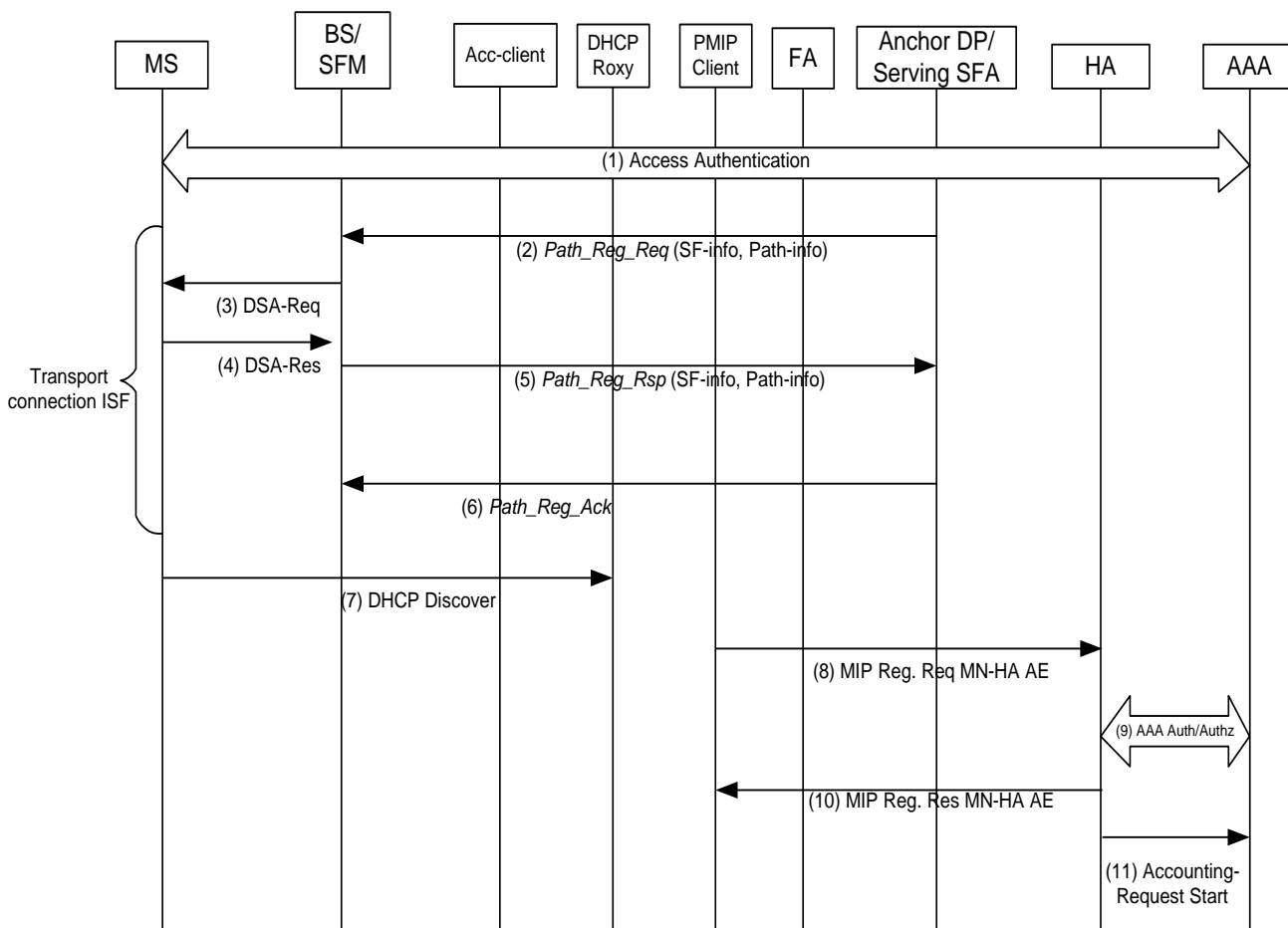


Figure 4-47 – Accounting Start Event in the CSN in Case of CMIP4



**Figure 4-48 – Accounting Start Event in the CSN in Case of PMIP4**

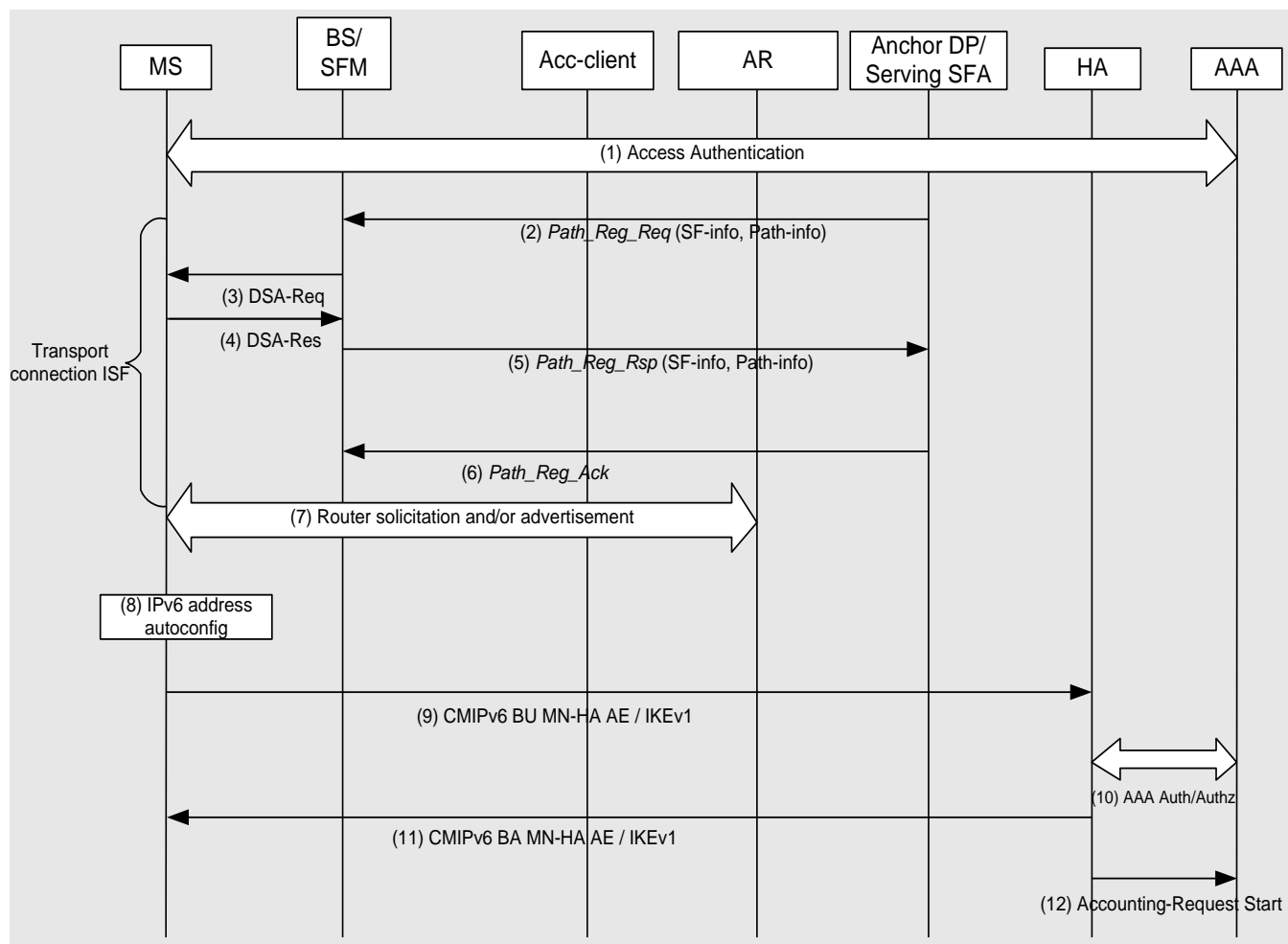


Figure 4-49 – Accounting Start Event in the CSN in Case of CMIP6



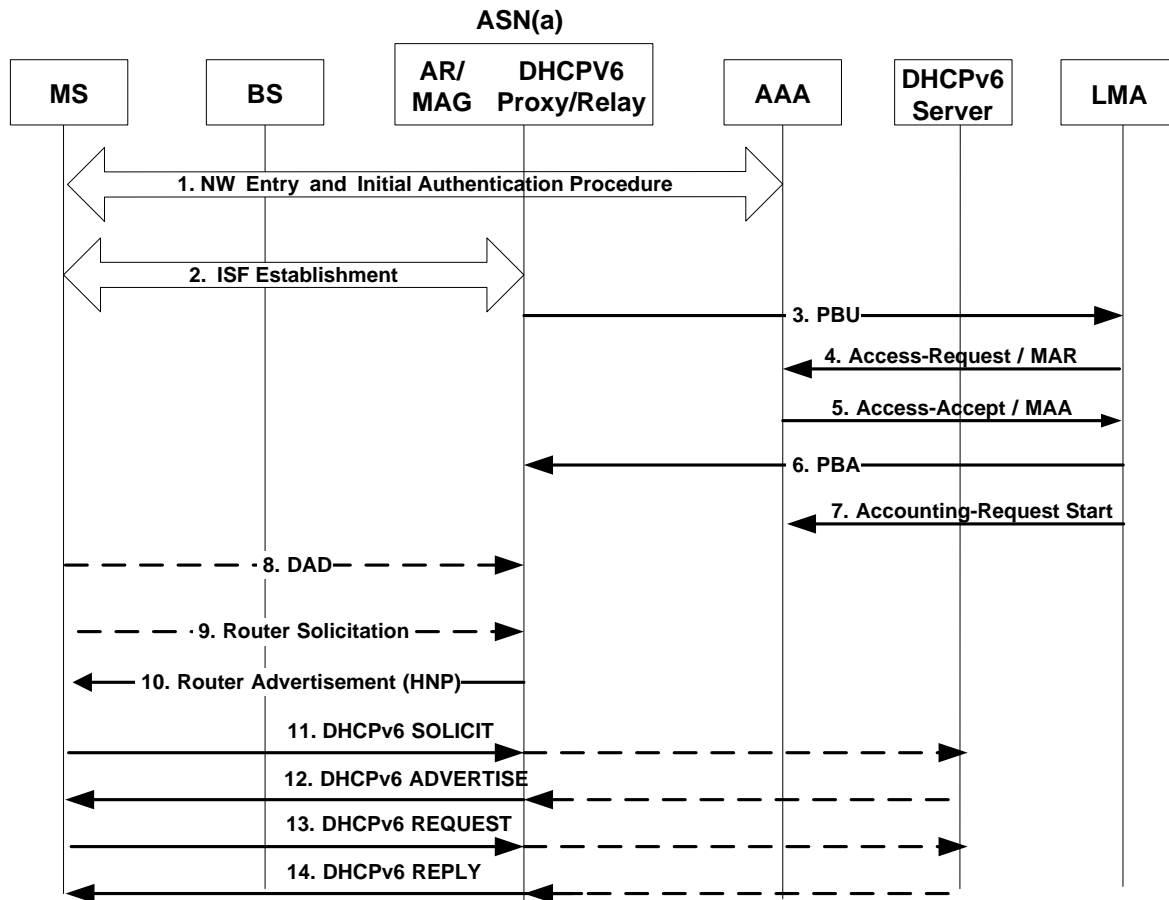


Figure 4-50 – Accounting Start Event in the CSN in Case of PMIPv6

## 4.5 Network Entry and Exit

### 4.5.1 MS-to-Network Initial Authentication Flow

#### 4.5.1.1 Single EAP

Figure 4-51 describes normative procedures for an initial MS network entry focusing on MS-to-Network EAP authentication process (single EAP) and MS 802.16e registration.

The BS and the Authenticator / ASN-GW SHALL be able to distinguish a new initial network entry with the same MAC address that is already used for an existing WiMAX session across R6 based on the R6\_Context\_ID value.

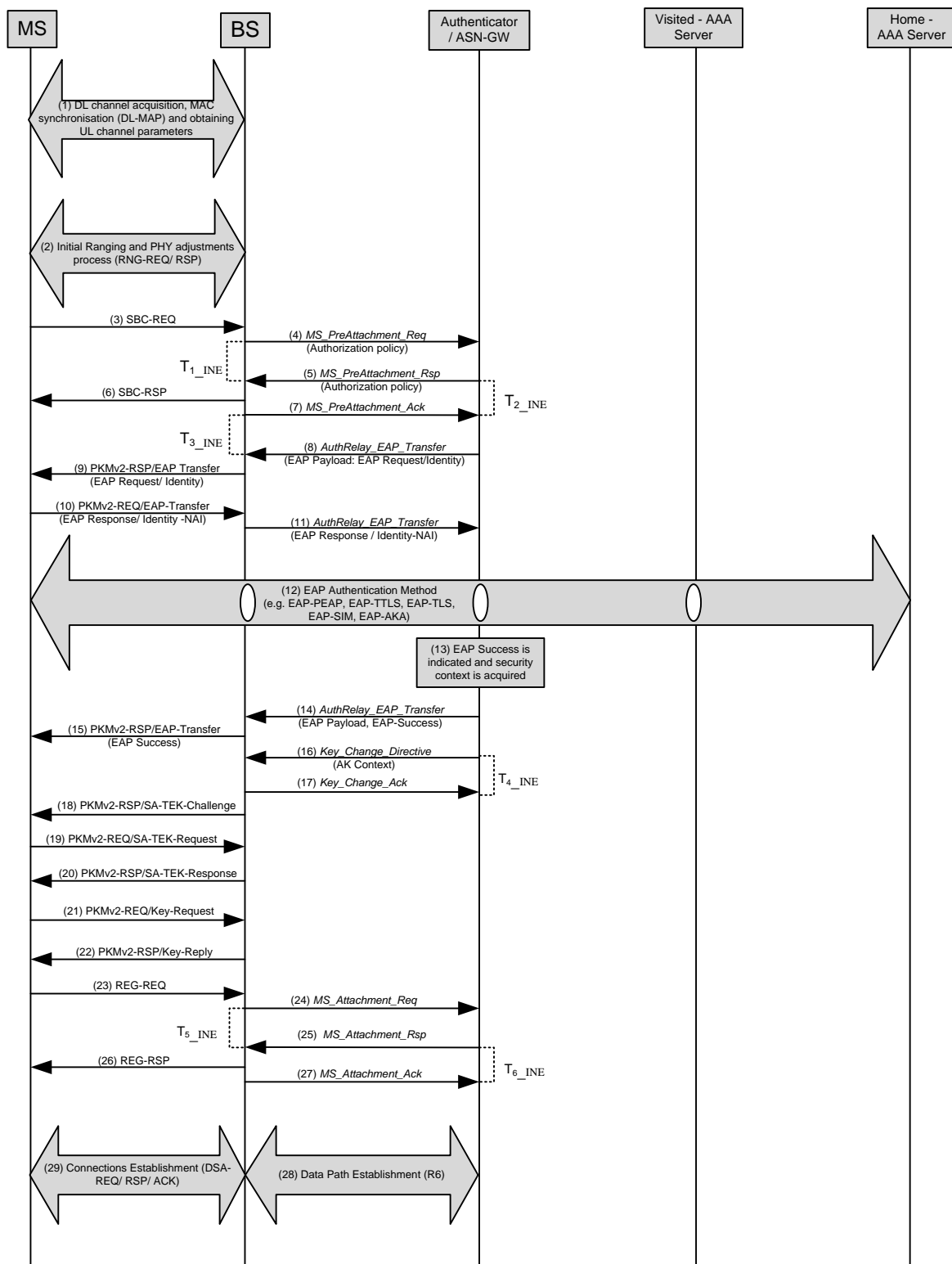


Figure 4-51 – MS Initial Network Entry (Single EAP)

802.16e MS Network Entry starts:

**STEP 1**

DL channel acquisition, MAC synchronization and obtaining UL channel parameters.

**STEP 2**

Initial Ranging round trips – RNG-REQ/ RNG-RSP message exchange. The MS performing initial network entry will perform CDMA ranging and after that will send RNG-REQ message without Serving BSID parameter thus indicating that it performs initial entry and not HO (as specified in [11] section 6.3.2.3.5).

**STEP 3**

MS sends an SBC-REQ message starting Basic Capabilities negotiation where MS and BS among other parameters negotiate the PKM protocol version, Authorization Policy and Message Authentication Code mode. MS MAY also include Visited NSP ID TLV in SBC-REQ to request the realm of the selected NSP.

**STEP 4**

The BS SHALL send *MS\_PreAttachment\_Req* message to its “default” Authenticator in order to inform it about the new MS entering the network.

The composition of this *MS\_PreAttachment\_Req* message is presented in Table 4-42:

**Table 4-42 – MS\_PreAttachment\_Req from BS to Authenticator**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>MS Security History	5.3.2.108	M	
>>Authorization Policy Support	5.3.2.21	M	Identifies the MS authorization policy.
>SBC Context	5.3.2.174	O	802.16e related MS session context.
>>Subscriber Transition Gaps	5.3.2.316	O	
>>Maximum Transmit Power	5.3.2.317	O	
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	O	
>>PKM Flow Control	5.3.2.319	O	
>>Maximum Number of Supported Security Associations	5.3.2.320	O	
>>Security Negotiation Parameters	5.3.2.321	O	
>>Extended Subheader Capability	5.3.2.325	O	
>>HO Trigger Metric Support	5.3.2.326	O	
>>Current Transmit Power	5.3.2.327	O	
>>OFDMA SS FFT Sizes	5.3.2.328	O	
>>OFDMA SS demodulator	5.3.2.329	O	

IE	Reference	M/O	Notes
>>OFDMA SS modulator	5.3.2.330	O	
>>The number of UL HARQ Channel	5.3.2.331	O	
>>OFDMA SS Permutation support	5.3.2.332	O	
>>OFDMA SS CINR Measurement Capability	5.3.2.333	O	
>>The number of DL HARQ Channels	5.3.2.334	O	
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	O	
>>OFDMA SS Uplink Power Control Support	5.3.2.336	O	
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	O	
>>OFDMA MAP Capability	5.3.2.338	O	
>>Uplink Control Channel Support	5.3.2.339	O	
>>OFDMA MS CSIT Capability	5.3.2.340	O	
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	O	
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	O	
>>OFDMA SS modulator for MIMO Support	5.3.2.343	O	
>>OFDMA Parameters Sets	5.3.2.50	O	
>>MS MAC Version	5.3.2.106	M	MS reported MAC Version. If the reported MAC Version is lower than 7 or is not present and the home NSP domain in the form of NAI provided by the MS does not correspond to NSP configured in the network, the MS is not supporting ND&S and SHALL be connected to a default NSP-ID, (i.e. a default NSP-ID is pre-configured by the NAP in the NAS – ASN-GW).
BS Info	5.3.2.26	M	Contains relevant Serving BS context in the nested IEs.
> BS ID	5.3.2.25	M	Serving BS ID.
>BS Location	5.3.2.425	O	Location info of the serving BS which may be described as Lat/Long/Sector/Carrier information of BS. NAS may pass this info to H-AAS which can use it to authorize stationary access services.

PKM protocol version and MAC mode are related to BS capabilities and SHOULD be enforced by BS as per network policy (there is no need to transfer these parameters to Authenticator).

The BS SHALL assign a value for this R6 context of the MS and SHALL include R6\_Context\_ID with this value. Assignment of the value is internal to the BS. The value SHALL uniquely identify this context of the MS at this BS (R6 context). The BS SHALL include the same R6\_Context\_ID value in all subsequent MS\_PreAttachment\_Req/\_Rsp/\_Ack, AR\_EAP\_Transfer/\_Start and Key\_Change\_Directive/\_Ack/\_Cnf messages belonging to the same R6 context at this BS.

If the resulting MS\_PreAttachment\_Rsp from the authenticator does not include an R6\_Context\_ID TLV, the BS SHALL assume that the authenticator does not support R6\_Context\_ID and SHALL not include R6\_Context\_ID in subsequent R6 messages for this R6 context.

If a duplicate-MAC case occurs at the same base station within a network where device authentication is always enforced, based on BS knowledge of the liveness of the active session, the BS MAY ignore the RNG-REQ of the new MS entry with the MS using the same MAC address.

#### STEP 5

Authenticator in the ASN/ASN-GW receiving MS\_PreAttachment\_Req creates a new context block related to this MSID and responds to BS with MS\_PreAttachment\_Rsp message. The composition of this message is presented in Table 4-43:

**Table 4-43 – MS\_PreAttachment\_Rsp from Authenticator to BS**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.
Failure Indication	5.3.2.69	O	
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
>Authenticator ID	5.3.2.19	O	Identifies the authenticator for the given MS. When this TLV is presented, BS SHALL use this Authenticator ID as a destination identifier for the subsequent transactions such as Auth Relay messages.
>MS Security History	5.3.2.108	M	
>>Authorization Policy Support	5.3.2.21	M	Identifies the MS authorization policy.
BS Info	5.3.2.26	M	Contains relevant Serving BS context in the nested IEs.
> BS ID	5.3.2.25	M	Serving BS ID.

#### STEP 6

The authenticator SHALL include R6\_Context\_ID in MS\_PreAttachment\_Rsp with the value set to the same value received from the BS in the MS\_PreAttachment\_Req message that initiated this R6 context.

If the MS\_PreAttachment\_Req message received from the BS did not include an R6\_Context\_ID TLV, the authenticator SHALL assume that this BS does not support R6\_Context\_ID and SHALL not include R6\_Context\_ID in any subsequent R6 message for this R6 context of the MS.

BS receiving SBC-REQ sends SBC-RSP message to MS enforcing the authentication framework policy (PKMv.2, single EAP, CMAC mode). If MS includes Visited NSP ID TLV in SBC-REQ, BS SHALL include Visited NSP Realm TLV in SBC-RSP.

The point in time when SBC-RSP is sent is an implementation decision of the BS: that is, it may be sent before or after performing the MS Pre-Attachment exchange with the Authenticator in the ASN/ASN-GW.

If the SBC Context is included in MS\_PreAttachment\_Req message from BS to authenticator, there are SBC Context parameters negotiated with authenticator. The BS should send SBC-RSP message to MS after performing the MS\_PreAttachment\_Req and MS\_PreAttachment\_Rsp exchange with the ASN/ASN GW Authenticator. Otherwise, the SBC-RSP may be sent to MS before the negotiation.

In the case MS does not receive SBC-RSP, it will retransmit SBC-REQ.

#### STEP 7

BS sends MS\_PreAttachment\_Ack message to the Authenticator (in ASN/ASN-GW) to confirm that SBC-RSP has been sent to MS. Note that this does not confirm that MS has successfully received SBC-RSP.

**Table 4-44 – MS\_PreAttachment\_Ack from BS to Authenticator**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.

#### STEP 8

The Authenticator (in ASN/ASN GW) initiates EAP authentication procedure with MS. The trigger for it - is the successful end of the MS Pre-Attachment transaction.

The Authenticator sends EAP Request/ Identity message over Authentication Relay protocol (*AR\_EAP\_Transfer*) to BS.

The composition of this message is presented in Table 4-45:

**Table 4-45 – AR\_EAP\_Transfer from Authenticator to BS (EAP initiation)**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.
EAP Payload	5.3.2.62	M	EAP message. In this step it SHALL include EAP Identity Request message.

Note that *AR\_EAP\_Transfer* message composition remains the same through the EAP authentication process with only difference in the content of the EAP Payload TLV (containing different EAP messages).

The R6\_Context\_ID value in all subsequent AR\_EAP\_Transfer messages SHALL be set to the same value received from the BS in the MS\_PreAttachment\_Req message that initiated this R6 context.

#### STEP 9

The BS relays the EAP Request/ Identity payload (received in *AR\_EAP\_Transfer* message) in the PKMv2-RSP/EAP-Transfer message to the MS.

#### STEP 10

MS responds with EAP Response/ Identity message providing NAI. This message is transferred to BS over PKMv2-REQ/EAP-Transfer message.

**STEP 11**

BS relays EAP payload received in PKMv2 EAP-Transfer to the Authenticator over Authentication Relay protocol (*AR\_EAP\_Transfer* message).

**STEP 12**

The Authenticator analyses the NAI provided by the MS Depending on the realm, EAP payload MAY be forwarded to the MS' Home AAA server via the Visited AAA server (using the provided NAI for resolving the Home-AAA server location). In order to deliver the EAP payload to the AAA server, the Authenticator forwards the EAP message via a collocated AAA client using RADIUS Access-Request packet or Diameter WDER command (EAP payload is encapsulated into “EAP message” attribute/AVP(s)).

The EAP authentication process (tunneling EAP authentication method) is performed between the MS and the Authentication server via the Authenticator in ASN/ASN-GW. BS provides “relay” of EAP payload from PKMv2 EAP-Transfer messages to *AR\_EAP\_Transfer* and vice versa. The Authenticator in ASN/ASN-GW acts in pass through mode (as described in [52]) and forwards the EAP messages received as a payload from the BS in *AR\_EAP\_Transfer* messages to the AAA server using RADIUS Access-Request packets or Diameter WDER commands and vice versa – transferring EAP payload from RADIUS Access-Challenge packets or Diameter WDEA commands to *AR\_EAP\_Transfer*. There can be multiple EAP message exchanges between the MS and AAA server.

The composition of RADIUS messages is presented in the section 5.4.1 and Diameter commands in section 5.5.1.1.

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

**STEP 13**

The Authenticator receives indication about the successful completion of EAP-based authentication, the MS authorization profile and the required security context (i.e., MSK key and its lifetime). It is done using RADIUS Access-Accept packet or Diameter WDEA command from AAA server with EAP-Success message encapsulated in “EAP message” attribute. In the case of EAP process failure, the Authenticator will receive RADIUS Access-Reject packet or Diameter WDEA command with EAP-Failure encapsulated in “EAP message” attribute.

The composition of RADIUS messages is presented in the section 5.4.1 and Diameter commands in section 5.5.1.1.

**STEP 14**

The Authenticator forwards EAP results (EAP-Success or EAP-Failure message) to BS as EAP Payload TLV in *AR\_EAP\_Transfer* message.

In the case of EAP-Success, if the NAS can confirm that the newly authenticated MS has successfully performed device authentication (i.e. if the MS-Authenticated attribute/AVP is supported by the NAS and is sent by the AAA), the NAS SHALL initiate MS network exit for any MS context using the same MAC address as the MS context that is newly authenticated by the Access-Accept or WDEA message received from the HAAA.

Otherwise, in the case of EAP-Success the NAS SHALL abort the new network entry and trigger MS network exit if there is an existing MS context using the same MAC address as the newly authenticated MS context for which the NAS can confirm that device authentication was performed at the time of network entry and hence the MAC address is authenticated.

If the NAS triggers MS network exit for any MS and an R6\_Context exists for this MS, the NAS SHALL include the R6\_Context\_ID value of this R6 Context in any *NetExit\_State\_Change\_Req/Rsp* message.

**STEP 15**

The BS relays EAP payload (received in *AR\_EAP\_Transfer* message) to the MS in PKMv2 EAP-Transfer/ PKM-RSP message (not protected by CMAC according to [11]). This message indicates the results of EAP authentication round to the Supplicant in the MS. Note that the BS does not relate to the content of EAP Payload – whether it is EAP-Success or EAP-Failure message. The BS continues waiting for the explicit indication of EAP authentication

completion from the Authenticator. MS is also waiting for PKMv2 SA-TEK-Challenge message from BS to proceed with PKMv2 3way handshake.

#### STEP 16

The Authenticator in ASN/ASN-GW sends *Key\_Change\_Directive* message to the BS to indicate completion of the EAP authentication process. The composition of this message is presented in Table 4-10:

This message informs the BS that it SHOULD proceed with PKMv2 3-way handshake (start the new key enforcement and Security Associations creation process).

*Key\_Change\_Directive* message SHOULD include AK Context parameter including the appropriate keying material – AK, key's context, etc.

The R6\_Context\_ID value in *Key\_Change\_Directive* SHALL be set to the same value received from the BS in the MS\_PreAttachment\_Req message that initiated this R6 context.

This specification does not define MS security properties (the number of SAs and their attributes) delivery from a Home AAA server to ASN and from an Authenticator to a BS. Instead, the single “default” SA (Primary SA) SHOULD be configured in a BS. (All the preprovisioned service flows should be associated with this “default” SA during service flow establishment process).

In the case authentication failure signal is received from the AAA server (RADIUS Access-Reject packet or Diameter WDEA command with EAP-Failure), the Authenticator may decide to restart EAP authentication process (by sending the new EAP Request Identity) or bring down the user. In the latter case, the Authenticator proceeds with MS Network Exit procedure.

#### STEP 17

BS receiving *Key\_Change\_Directive* from Authenticator will acknowledge it by *Key\_Change\_Ack* message.

The BS SHOULD initiate MS network exit for any existing MS context that is using the same MAC address as the one that is newly authenticated as indicated by the *Key\_Change\_Directive* message received from the ASN-GW, if for the existing MS context a different authenticator than for the newly authenticated MS context is used (otherwise the Authenticator will trigger MS network exit). If the BS triggers such MS network exit, it SHALL include the R6\_Context\_ID value of this R6 Context in the corresponding NetExit\_State\_Change\_Req/Rsp messages.

#### STEP 18, 19, 20

PKMv2 3-way handshake (SA-TEK-Challenge/Request/Response exchange) is conducted between BS and MS to verify the AK to be used and to establish the Security Association(s) pre-provisioned for the MS (WiMAX Rel.1 assumes the “default” SA-Descriptor identifying the primary SA to be provisioned in a BS).

The BS SHALL ensure that PKMv2 3way handshake is indeed successfully completed and the new PMK/AK is enforced by the MS – i.e., the BS should receive and verify a MAC management message from the MS signed by CMAC derived from the new AK. Said MAC management message may be the one described in step 21 (Key Request/Reply) or the one in step 23 (REG-REQ/RSP).

When BS recognizes the completion of PKMv2 3way handshake process (success or failure), it SHALL indicate this event to Authenticator. This indication is described in the step 24.

If the BS recognizes after successful completion of the PKMv2 handshake that the MAC address of the new entry is already part of another authenticated MS context and the latter MS is using a different authenticator than the new entry, the BS SHALL initiate network exit for the latter MS (if the same authenticator is used, the authenticator is in charge of triggering network exit for any overlapping MAC. If the BS triggers such MS network exit, it SHALL include the R6\_Context\_ID value of this R6 Context in the corresponding NetExit\_State\_Change\_Req/Rsp messages.

#### STEP 21, 22

MS acquires the valid TEK keys using PKMv2 Key-Request/ Reply exchange between MS and BS for each SA (This step is repeated for each SA).



## STEP 23

When PKMv2 3-way handshake is completed, MS proceeds with 802.16e Registration procedure by sending REG-REQ message as specified in 6.3.2.3.7 of [11]. This message will carry the MS supported capabilities (such as CS capabilities, Mobility parameters and Handover support, etc.).

## STEP 24

In the case the BS detects successful PKMv.2 3WHS completion and successfully validates CMAC tuple of REG-REQ message from the MS, the BS sends *MS\_Attachment\_Req* message to the Authenticator including also the MS REG Context parameters. The composition of this message is presented in Table 4-46:

**Table 4-46 – MS\_Attachment\_Req from BS to Authenticator**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
> REG Context	5.3.2.144	O	SHALL be included if it is received from MS in REG-REQ and as supported by the BS.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per Frame Support	5.3.2.296	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
BS Info	5.3.2.26	M	
> BS ID	5.3.2.25	M	Serving BS ID
>Reattachment Zone	5.3.2.424	O	Included if configured at BS. NAS can use this info for fixed and nomadic access to create the static Reattachment Zone list in the MS info used to restrict MS mobility.

- 1
- 2 In case the BS detects 3-way handshake failure, it SHALL update the Authenticator by sending Key\_Change\_Cnf
- 3 message with Key Change Indicator TLV set to indicate “failure”. The Authenticator responds with
- 4 Key\_Change\_Ack message to the BS and initiates MS Network Exit (as described in section 4.5.2).
- 5 **STEP 25**
- 6 ASN/ASN GW Authenticator receiving *MS\_Attachment\_Req* message, responds to BS with *MS\_Attachment\_Rsp*
- 7 message. The composition of this message is presented in Table 4-47:

1

**Table 4-47 – MS\_Attachment\_Rsp from Authenticator to BS**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
MS Info	5.3.2.103	O	Contains MS-related context in the nested IEs.
> REG Context	5.3.2.144	O	Identifies the MS REG Context parameters as enforced by the Authenticator. SHALL be included if it is included in the MS_Attachment_Req message.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Total Number of Provisioned Service Flows	5.3.2.295	O	
>>Maximum MAC Data per Frame Support	5.3.2.296	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>Mobility Access Classifier	5.3.2.423	O	Indicates the mobility access classification of the subscriber. It SHALL be included if it was received from the H-AAA during authentication and its value is Fixed or Nomadic.
>Reattachment Zone	5.3.2.424	O	Indicates the list of BS IDs allowed for reattachment. It SHALL be included if mobility access classifier is included. The list is generated by the NAS using BSID and Reattachment Zone info received in the BS Info in the MS_Attachment_Req or by some other means (e.g. pre-provisioned).
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

# 1 **STEP 26**

2 The BS sends REG-RSP message to MS as specified in 6.3.2.3.8 of [11] formatting the appropriate parameters  
3 (from BS policy and/or ASN/ASN GW Authenticator response).

4 The point in time when REG-RSP is sent is an implementation decision of the BS; that is, it may be sent before or  
5 after performing the *MS\_Attachment\_Req* and *MS\_Attachment\_Rsp* exchange with the ASN/ASN GW  
6 Authenticator.

If the REG Context is included in *MS\_Attachment\_Req* message from BS to authenticator, there are REG Context parameters negotiated with authenticator. The BS SHALL send REG-RSP message to MS after performing the *MS\_Attachment\_Req* and *MS\_Attachment\_Rsp* exchange with the ASN/ASN GW Authenticator. Otherwise, the REG-RSP may be sent to MS before the negotiation. In case the MS does not receive REG-RSP, it will retransmit REG-REQ.

#### STEP 27

The BS sends *MS\_Attachment\_Ack* message to the Authenticator in the ASN/ASN-GW indicating that *MS\_Attachment\_Rsp* message from the ASN/ASN GW Authenticator has been received and REG-RSP message has been sent to MS. This message serves as a trigger to the ASN/ASN GW Authenticator to instigate the process of pre-provisioned service flows establishment.

#### STEP 28, 29

ASN/ASN-GW triggers SFA to create the Initial service flow (ISF) and optionally other pre-provisioned service flows. The BS SHALL use the Anchor DPF ID used during this procedure for subsequent operations such as Data Path Release, with the Anchor DPF, for the given MS.

Note: After the creation of ISF, and as long as the IP session (s) is/are not established for the MS, it is operator/network policy when to initiate Network exit for the MS as specified in section 4.5.2.

### 4.5.1.2 Error Handling During Initial Network Entry

#### 4.5.1.2.1 Timers and Timing Considerations

This section identifies the timer that the entities participating in the Initial Network Entry procedure SHALL use. The Initial Network Entry procedure utilizes seven timers:

- $T_{1\_INE}$ : is started by a BS upon sending an *MS\_PreAttachment\_Req* (Authorization policy support). It is stopped upon receiving a corresponding *MS\_PreAttachment\_Rsp*.
- $T_{2\_INE}$ : is started when an Authenticator sends an *MS\_PreAttachment\_Rsp* and is stopped upon receiving a corresponding *MS\_PreAttachment\_Ack*.
- $T_{3\_INE}$ : is started by the BS when *MS\_PreAttachment\_Ack* is sent and Authorization Policy is negotiated. It is stopped upon receiving *AR\_EAP\_Transfer*.
- $T_{4\_INE}$ : is started by the Authenticator when it sends a *Key\_Change\_Directive* message and is stopped upon receiving the *Key\_Change\_Ack*.
- $T_{5\_INE}$ : is started by a BS upon sending an *MS\_Attachment\_Req*. It is stopped upon receiving a corresponding *MS\_Attachment\_Rsp*.
- $T_{6\_INE}$ : is started when an Authenticator sends an *MS\_Attachment\_Rsp* and is stopped upon receiving a corresponding *MS\_Attachment\_Ack*.

Table 4-48 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-48 – Timer Values for Initial Network Entry Procedure**

Timer	Default Values (msec)	Criteria	Maximum Timer Value (msec)
$T_{1\_INE}$	TBD		TBD
$T_{2\_INE}$	TBD		TBD
$T_{3\_INE}$	TBD		TBD
$T_{4\_INE}$	TBD		TBD

Timer	Default Values (msec)	Criteria	Maximum Timer Value (msec)
T <sub>5_INE</sub>	TBD		TBD
T <sub>6_INE</sub>	TBD		TBD

#### 4.5.1.2.2 Handling Error Conditions

Table 4-49 lists the behavior for various error conditions during Initial Network Entry:

**Table 4-49 – Initial Network Entry – Handling Error Conditions**

	Failure Case	Action
1	Auth failure at the Authenticator.	The authenticator initiates Network Exit procedure by sending <i>NetExit_MS_State_Change_Req</i> with Action Code set to 0xfffe which indicates initial authentication failure as described in the section 4.5.2.1.2.4.
2	<i>MS_PreAttachment_Req</i> or <i>MS_Attachment_Req</i> messages not understood by the Authenticator (decode error, corrupted packet etc.).	Send <i>MS_PreAttachment_Rsp</i> (or <i>MS_Attachment_Rsp</i> correspondingly) with Failure Indication TLV.
3	<i>MS_PreAttachment_Rsp</i> or <i>MS_PreAttachment_Ack</i> 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 4.5.1.2.4).
5	MS dropped call at the BS during call setup.	Initiate to the peer entity using procedure described in the MS Network Exit section 4.5.1.2.4.
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 <i>Path_Dereg_Req</i> .
8	<i>Path_Dereg_Req</i> received for a MS or Data Path that does not exist.	Respond with <i>Path_Dereg_Rsp</i> 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 <i>MS_PreAttachment_Req</i> message for the same MSID with a new Transaction ID value. Authenticator should restart the transaction - respond with <i>MS_PreAttachment_Rsp</i> and reset T <sub>2_INE</sub> 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 <i>MS_Attachment_Req</i> message for the same MSID with a new Transaction ID value. Authenticator should restart the transaction - respond with <i>MS_Attachment_Rsp</i> and reset T <sub>6_INE</sub> timer.

	Failure Case	Action
11	BS detects PKMv2 3way handshake failure for any reason.	BS sends <i>Key_Change_Cnf</i> message with Key Change Indicator TLV set to indicate “failure”. Authenticator responds with <i>Key_Change_Ack</i> message and initiates MS Network Exit (as described in the section 4.5.1.2.4).

#### 4.5.1.2.3 Timer Expiry

Table 4-50 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 4-50.

**Table 4-50 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T <sub>1_INE</sub>	BS	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T <sub>2_INE</sub>	Authenticator	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T <sub>3_INE</sub>	BS	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T <sub>4_INE</sub>	Authenticator	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T <sub>5_INE</sub>	BS	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T <sub>6_INE</sub>	Authenticator	Initiate MS Network Exit (as described in section 4.5.2.1.1).

#### 4.5.1.2.4 Duplicate MAC address handling

During initial network entry, it may occur that an MS performs initial network entry with using the same MAC address that is already bound to an existing and currently active WiMAX session.

This specification does not allow different MSes using the same MAC address to be in the network in parallel, that is, for a specific MAC address there can only be one successfully authenticated WiMAX session at the same time.

A new initial network entry with a MAC address that is already bound to an active WiMAX session is not necessarily indicating a misbehaving MS but may for example be launched by a MS that was reset while being in idle mode. In this case the network may not be aware of the real MS status and may still consider the idle MS as being a valid session. Hence, the MS has to be allowed a new initial network entry after successful authentication and authorization.

A MS performing initial network entry and using a MAC address that is already bound to an existing and active WiMAX session will be able to perform the network entry steps in parallel to the existing session, up to the point where the new entry attempt is either authenticated and authorized by the CSN AAA server by sending EAP-Success, or not. In the successful case, network exit will be triggered for the already existing WiMAX session with the same MAC address, and the new network entry will be successful. This is to allow a MS to re-enter the network in case of any fatal state loss at the MS side, while cleaning up the old context.

If the unsuccessful case (EAP-Failure sent by the AAA), the new entry attempt will fail and the current session will continue as normal.

Within the ASN, uniqueness of the parallel sessions bound to the same MAC address is ensured by the R6\_Context\_ID value. The BS and the ASN-GW that are involved in the new initial network entry procedure must distinguish the parallel sessions for the same MAC value across R6 based on the combination of the MAC address (MS-ID) and the R6\_Context\_ID.

As a result, it is not possible for a misbehaving MS to negatively impact or terminate ongoing WiMAX sessions of legitimate MSes through MAC address spoofing, without proper authentication based on a valid subscription. On the contrary, for any misbehaving or malfunctioning MS the NAP and NSP are able to clearly identify the related subscription and can take appropriate measures to prevent further misuse.

An additional measure for the NSP operator to ensure the correctness of MS MAC addresses is to enforce device authentication during initial network entry. When required to perform device authentication based on the device certificate, the MS would not be able to perform initial network entry when using a MAC address different from the one being part of the signed device certificate.

If a duplicate-MAC case occurs at the same base station within a network where device authentication is always enforced, based on BS knowledge of the liveness of the active session, the BS MAY ignore the RNG-REQ of the new MS entry with the MS using the same MAC address.

For an emergency network entry or an active session that has been created as the result of an emergency network entry, the actual policy in a duplicate-MAC case for whether the new entry will be denied or the already active session will be terminated in favor of the new entry, is up to the CSN operator's policy. This will depend on the local regulatory environment.

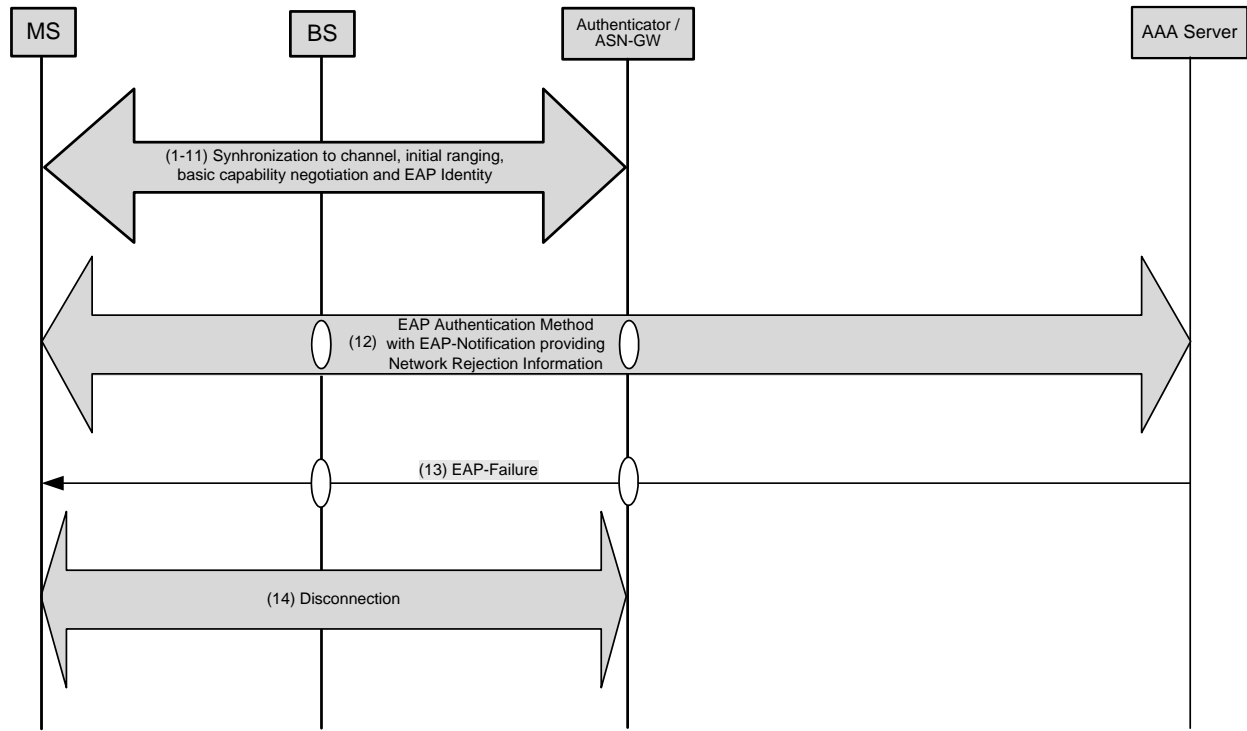
#### **4.5.1.3 Network Rejection Procedure**

Figure 4-52 describes the normative procedure for the Network Rejection procedure initiated during the EAP authentication process. This procedure allows Visited and Home Networks to provide the rejection reason when the MS is being denied access through this Network, such that the MS can act in a suitable manner.

When the Network Rejection is triggered, the EAP Notification Request is transmitted to the MS during the EAP authentication, in order to deliver the Network Rejection Information. Note that the EAP Notification Request can be issued at any time after EMSK is computed when there is no outstanding Request, prior to completion of an EAP authentication method as defined in the Section 5.2 of [56]. After disconnection caused by the Network Rejection Procedure, the MS SHALL act according to the Rejection Information that was delivered to it during the authentication failure procedure.

The Rejection Information includes a Rejection Code as defined in sub-clause 4.12.7 respectively 5.8.3. The Rejection Codes are classified into various Rejection Classes that provide information on handling required at the MS. When the AAA server triggers the Network Rejection, the Rejection Information SHALL be integrity protected using the RMAC defined in sub-clause 5.8.8. Since the EMSK (Extended Master Session Key) is required to calculate the RMAC value used to protect the Network Rejection Information, it SHALL be successfully derived by the AAA before sending the EAP-Notification Request. After receiving the EAP-Notification Request containing the Network Rejection Information and deriving the EMSK at the MS side, the MS SHALL perform the integrity check over the Network Rejection Information. If the RMAC is not included in the Network Rejection Information or the integrity check fails, then the MS SHALL ignore the received Network Rejection Information.





**Figure 4-52 – Network Rejection Procedure during EAP**

### STEP 1 - 11

See STEP1 – STEP11 described in sub-clause 4.5.1.1.

### STEP 12

The Authenticator in the ASN/ASN-GW acts in a pass through mode (as described in 4.5.1.1) and forwards the EAP messages received as a payload from the BS in AR\_EAP\_Transfer messages to the AAA server using RADIUS Access-Request messages and vice versa. There can be multiple EAP message exchanges between the MS and AAA server.

When the Visited NSP decides to initiate the Network Rejection with the MS without involvement of the Home CSN (either because it has no roaming agreement with the Home NSP or it has to do the rejection for other reasons), the Visited NSP SHALL handle the authentication/authorization of the MS by not forwarding any AAA messages towards the Home NSP. Furthermore, the VAAA SHALL negotiate the use of EAP-TLS with the MS.

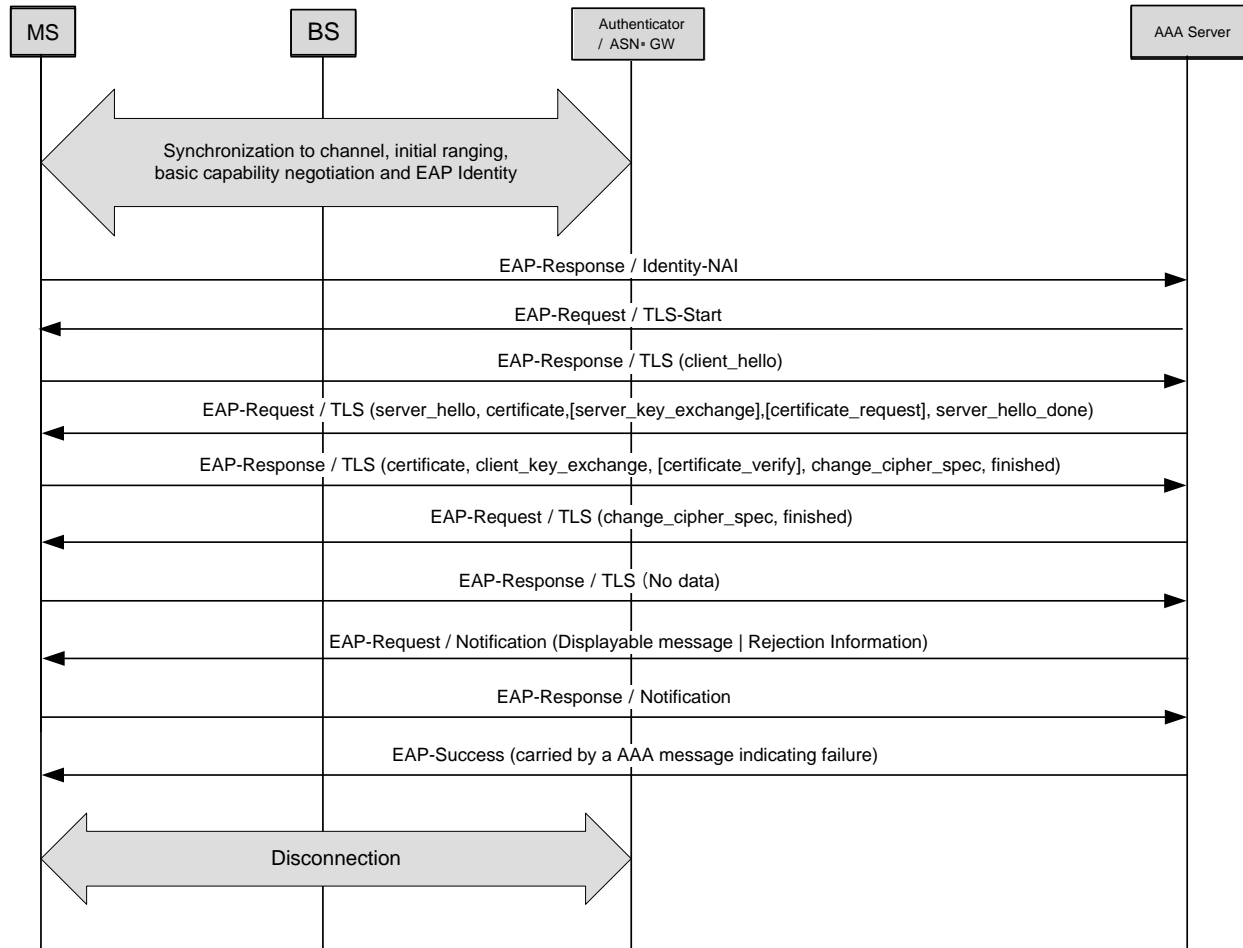
The local AAA server includes its own certificate with the EAP-TLS server\_hello message. When the MS receives a AAA server certificate, the MS SHALL validate the AAA server certificate and act as defined in the section 4.4.1.2. If MS receives network rejection information from a VNSP, different than the one chosen during ND&S, the MS SHOULD ignore the network rejection.

When the Home AAA Server receives an EAP payload forwarded by the Visited AAA Server, the Home AAA server may trigger the Network Rejection Procedure for a number of reasons, for instance:

- Network overload;
- MS equipment feature conformance;
- Fixed or nomadic network;
- Subscription related problems;

- Illegal or misbehaving handsets;
- Location specific subscriptions.

If the AAA Server decides to trigger the Network Rejection, it transmits the EAP-Request/Notification containing the Network Rejection Information after deriving the EMSK, and prior to sending the EAP result. For the Network Rejection, the AAA Server completes the EAP conversation with EAP-Success, if the authentication succeeds during the EAP conversation. Figure 4-53 ~ Figure 4-56 illustrate possible Network Rejection flow examples for the EAP-TLS, EAP-TTLS, and EAP-AKA, respectively.



**Figure 4-53 – Network Rejection Procedure for EAP-TLS**

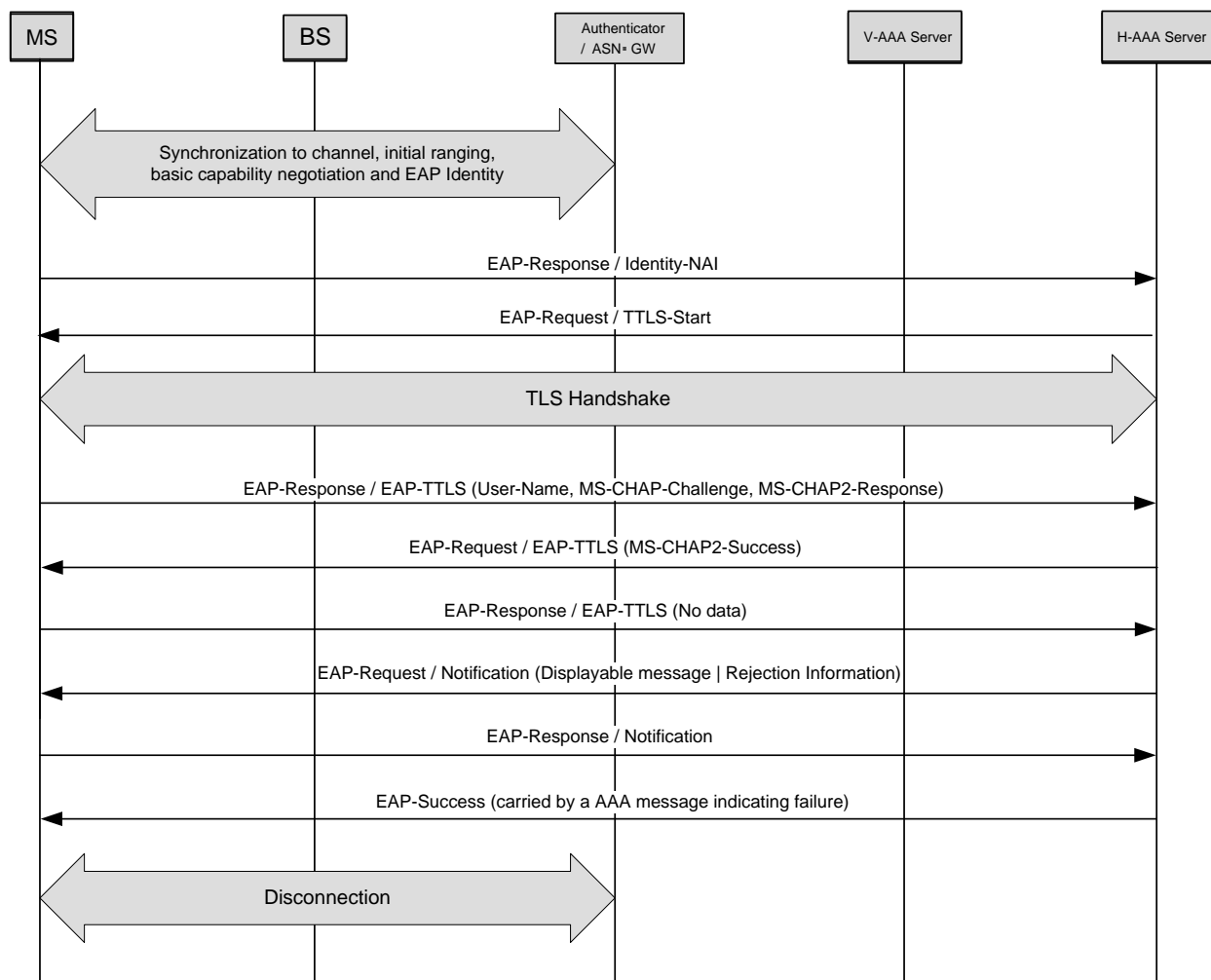
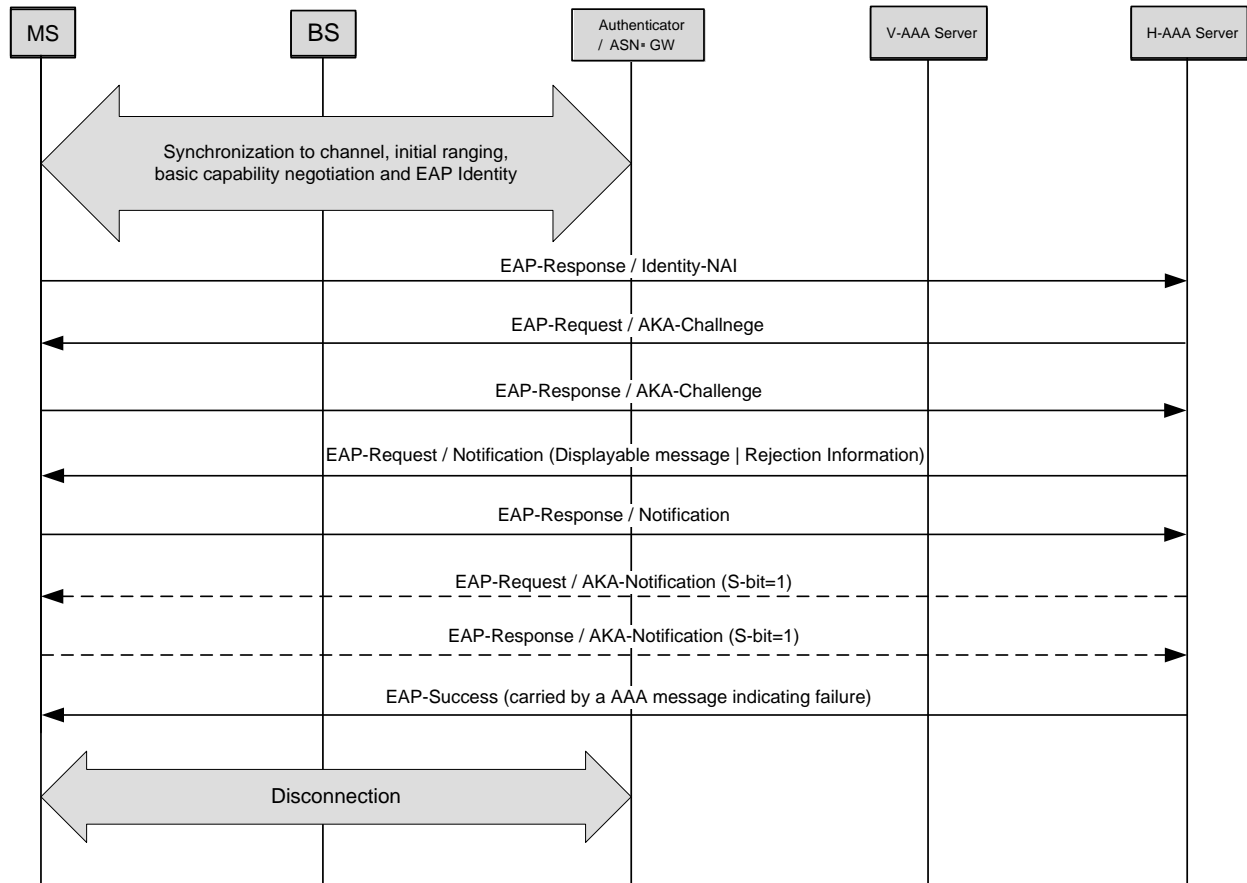


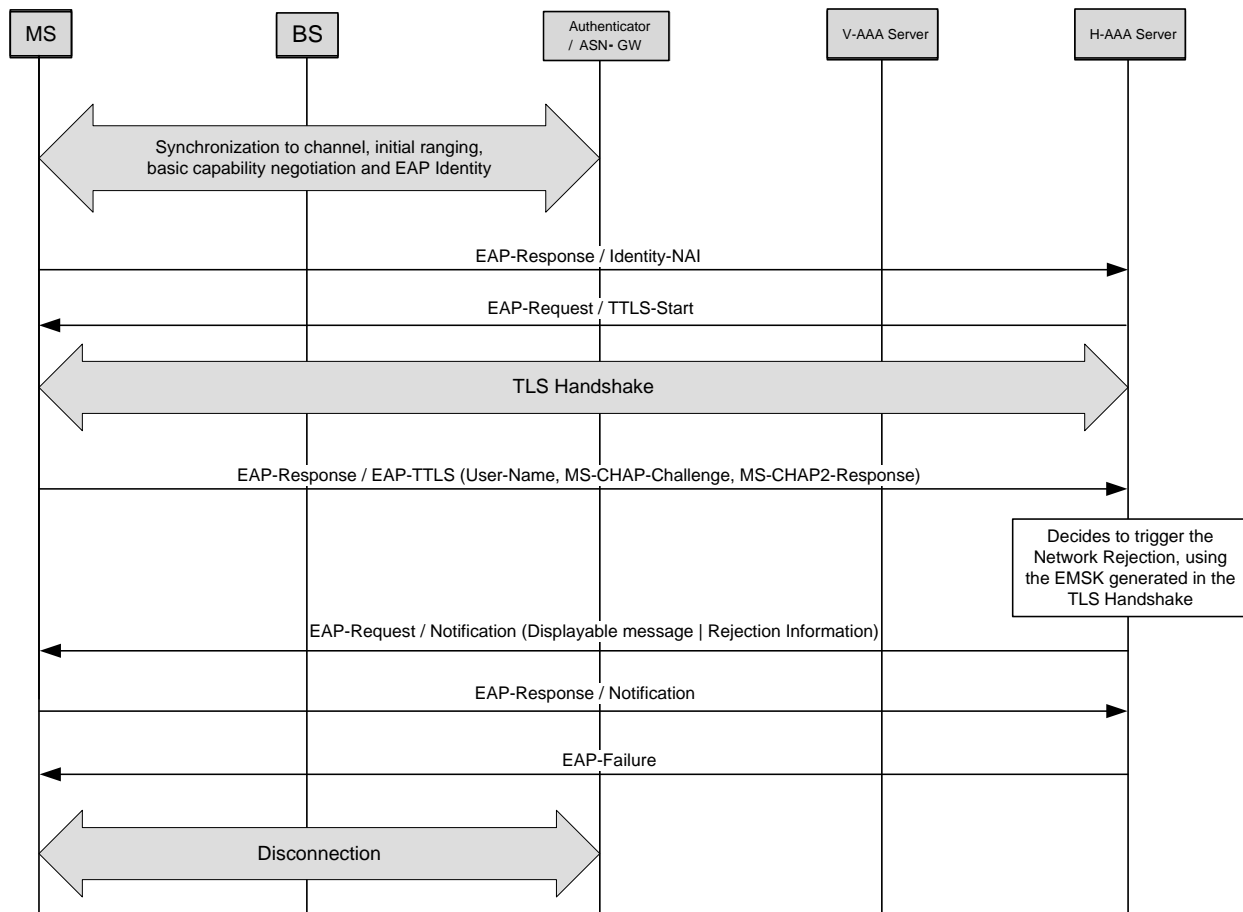
Figure 4-54 – Network Rejection Procedure for EAP-TTLS



**Figure 4-55 – Network Rejection Procedure for EAP-AKA**

During the Network Rejection procedure with EAP-AKA, if AKA-Notification is used for the success result indication, EAP-Notification SHALL be sent prior to the AKA-Notification, according to [16]. Note that, however, the use of the AKA-Notification is optional and hence it is illustrated in the dotted line in the figure.

The Network Rejection is basically based on the authentication success, to guarantee a successful calculation of the EMSK. Even if the authentication fails, however, if the EMSK was successfully generated during the EAP conversation, the AAA Server MAY trigger the Network Rejection by sending the EAP-Notification protected with RMAC, which is followed by the EAP-Failure. Figure 4-56 shows an example of the Network Rejection with the EAP-Failure.



**Figure 4-56 – Network Rejection Procedure in case of EAP-TTLS phase 2 Failure**

Figure 4-56 describes the Network Rejection procedure for the EAP-TTLS, which MAY be utilized by the HAAA when the authentication failure occurs during the EAP-TTLS phase 2. Although the authentication failure results in EAP-Failure, the Network Rejection is possible, since the EMSK can be generated in the phase 1, i.e. TLS handshake process. In order to trigger the Network Rejection, the HAAA transmits the Network Rejection Information via EAP-Notification Request protected by RMAC, prior to sending the final EAP-Failure message. The MS SHALL comply with the received Network Rejection Information, if the RMAC check succeeds using the EMSK generated at the MS side.

Irrespective of the EAP method being executed, if the Home AAA (or the Visited AAA as well) cannot derive the EMSK in the authentication process, it will not deliver the Network Rejection Information using the EAP-Notification.

### STEP 13

The AAA server issues the EAP-Success or EAP-Failure to complete the EAP conversation carried either by RADIUS Access-Reject or by Diameter WDEA with result code indicating failure. When the EAP conversation is completed with the EAP-Success, even though this EAP-Success indicates successful authentication (for example as a result of successful EAP-TLS authentication), MS determines the network access authorization result from the received EAP-Notification, and ASN makes the same determination from the received AAA message.

### STEP 14

The MS, BS, and the Authenticator perform the disconnection procedure as defined in [1].

#### 4.5.1.3.1 Network Rejection Information

The Network Rejection Information is coded as a TLV described in sub-clause 4.12.7 respectively 5.8.3. The Network Rejection Information TLV is passed to the MS in Type-Data field of the EAP-Notification Request message.

Note: The contents of this TLV will not be human readable, and therefore should not be displayed to the user without translation, for appropriate user response.

The Network Rejection Information includes the Rejection Code, a hint in case emergency network entry is not supported, and optionally information regarding the Allowed BSs. A Rejection Class is a group of Rejection Codes that have a common MS handling in terms of Security Category, Rejection duration/criteria, Applicability for Visited/Home AAA and scope of rejection.

The MS is allowed to perform an emergency network entry even if the Rejection Duration/Criteria has not been met. If emergency network entry is not supported by the network when the Rejection Duration/Criteria has not been met for a specific rejection, the network SHOULD indicate this to the MS by adding an Emergency Services Override TLV to the Network Rejection Information.

When a MS is rejected from all the NSPs connected through a NAP, the MS may continue to verify which NSP are available through other BSs advertising the same NAP ID.

#### 4.5.1.3.2 Rejection Classes

The following provides information on the handling required at the MS when receiving a Rejection Code from each of Rejection Class.

Rejection Class	Rejection Duration/Criteria	Applicability of Visited/Home AAA	Scope of Rejection
A	Until Manual Retry	Home AAA	All NAPs
B	Until Manual Retry	Visited/Home AAA	V-NSP
C	Until Power Cycle	Home AAA	All NAPs
D	Until Power Cycle	Visited/Home AAA	V-NSP
E	Until Timer Expiry	Home AAA	All NAPs
F	Until Timer Expiry	Visited/Home AAA	V-NSP
G	Until Location Criteria met	Home AAA	All NAPs
H	Until Location Criteria met	Visited/Home AAA	V-NSP
I	Until Device is upgraded or until CVS Timer Expiry	Home AAA	V-NSP
J	Until Device is upgraded or until CVS Timer Expiry	Visited AAA	V-NSP
K	Until Device is upgraded or until CVS Timer Expiry	Home AAA	H-NSP

#### Network Rejection Criteria

The Rejection Duration/Criteria indicates what type of criteria needs to be met before the MS is again allowed to access the network.

If the MS receives the Rejection Duration/Criteria indicating “Until Manual Retry”, the MS SHALL NOT access a network with the “Scope of Rejection” until the user manually initiates the reconnection, unless the access relates to an Emergency Service. If the user manually initiates the reconnection within 3 seconds after being rejected by the Network, the MS SHALL NOT attempt to access the network before the 3 seconds timer expired.

Note: The intention behind the use of the term “manually initiates the reconnection” is that the device is not autonomously reconnecting to the network, and ideally requires the user to press the connection button on the device for example.

If the MS receives the Rejection Duration/Criteria indicating “Until Power Cycle”, the MS SHALL NOT access a network with the “Scope of Rejection” until the MS has been manually power cycled, unless the access relates to an Emergency Service.

Note: The intention behind the use of the term “manually power cycled” is that the device is not autonomously reconnecting to the network, and ideally requires the user to turn off and on the WiMAX RF power. For some devices similar to a cellular phone, this is achieved when the whole terminal is power cycled. On the other hand, for some devices like a USB dongle or a modem integrated into a laptop platform, this is achieved when the RF module of the terminal is power cycled by the user.

If the MS receives the Rejection Duration/Criteria indicating “Until Timer Expiry”, the MS SHALL NOT access a network with the “Scope of Rejection” until a Network Rejection Timer associated to the rejection has expired, unless the access relates to an Emergency Service. The Network Rejection Timer is set to 5 minute for the first unsuccessful attempt for access through NSP within the “Scope of Rejection”. For each subsequent unsuccessful attempt for access through an NSP within the “Scope of Rejection” the MS SHALL double the Network Rejection Timer. The maximum value of the Network Rejection Timer SHALL be 6 hours. When the MS successfully registers through an NSP with the “Scope of Rejection” the MS SHALL reset the start value of the Network Rejection Timer.

If the MS receives the Rejection Duration/Criteria indicating “Until Device is upgraded or until CVS Timer Expiry”, the MS SHALL NOT access a network with the “Scope of Rejection” until either the device is upgraded, or until a Network Rejection Timer associated to the rejection has expired, unless the access relates to an Emergency Service and the Emergency Override is set to “Yes”. The CVS Network Rejection Timer is set to 1 week for the first unsuccessful attempt for access through NSP within the “Scope of Rejection”. For each subsequent unsuccessful attempt for access through an NSP within the “Scope of Rejection” the MS SHALL double the CVS Network Rejection Timer. The maximum value of the CVS Network Rejection Timer SHALL be 4 weeks. When the MS successfully registers through an NSP with the “Scope of Rejection” the MS SHALL reset the start value of the Network Rejection Timer.

If the MS receives the Rejection Duration/Criteria indicating “Until Location Criteria met”, the MS SHALL NOT access a network with the “Scope of Rejection” until the MS has moved to a BS that falls within the Allowed Location Information in the Network Rejection Information associated to the rejection has expired, unless the access relates to an Emergency Service and the Emergency Override is set to “Yes”. If no Allowed Location Information is included in the Network Rejection Information the MS SHALL only treat the current BS as Rejected through the Network Rejection procedure, regardless of the value of the “Scope of Rejection”. Whenever the Network Rejection occurs with Rejection Duration/Criteria indicating “Until Location Criteria met”, the previous restriction rule is superseded by the new rule received in the recent Rejection Information. The Location Restriction imposed by the Network Rejection with the Rejection Duration/Criteria indicating “Until Location Criteria met” is released when the MS is manually power cycled by the User.

#### ***Applicability of Visited/Home AAA***

If the MS receives a Rejection code from a Rejection Class from the Visited AAA where the Applicability is limited to the Home AAA, the MS SHALL ignore the Network Rejection Information. That means, the Visited AAA can reject the MS only from itself, not from other NSPs including the Home NSP.

#### ***Scope of the Rejection***

The Scope of the Rejection indicates whether the Rejection relates to the Visited NSP or to the Home NSP. If the MS has been rejected from each of the NSPs connected to a NAP, the MS SHALL NOT attempt to access the NAP whilst the Rejection Criteria/Duration remains. Note that rejection from V-NSP is limited to its role as V-NSP and does not prohibit the MS to try and obtain subscription from this NSP.

### **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.

#### **4.5.2.1 Normal Mode**

In the normal mode, considering MS exiting network entry, the related network entities will release the related data paths, resources and delete the MS contexts.

The scenarios mainly include MS powering down, resource blocking, fault, or changing service strategy of network side.



#### 4.5.2.1.1 MS Triggered Network Exit

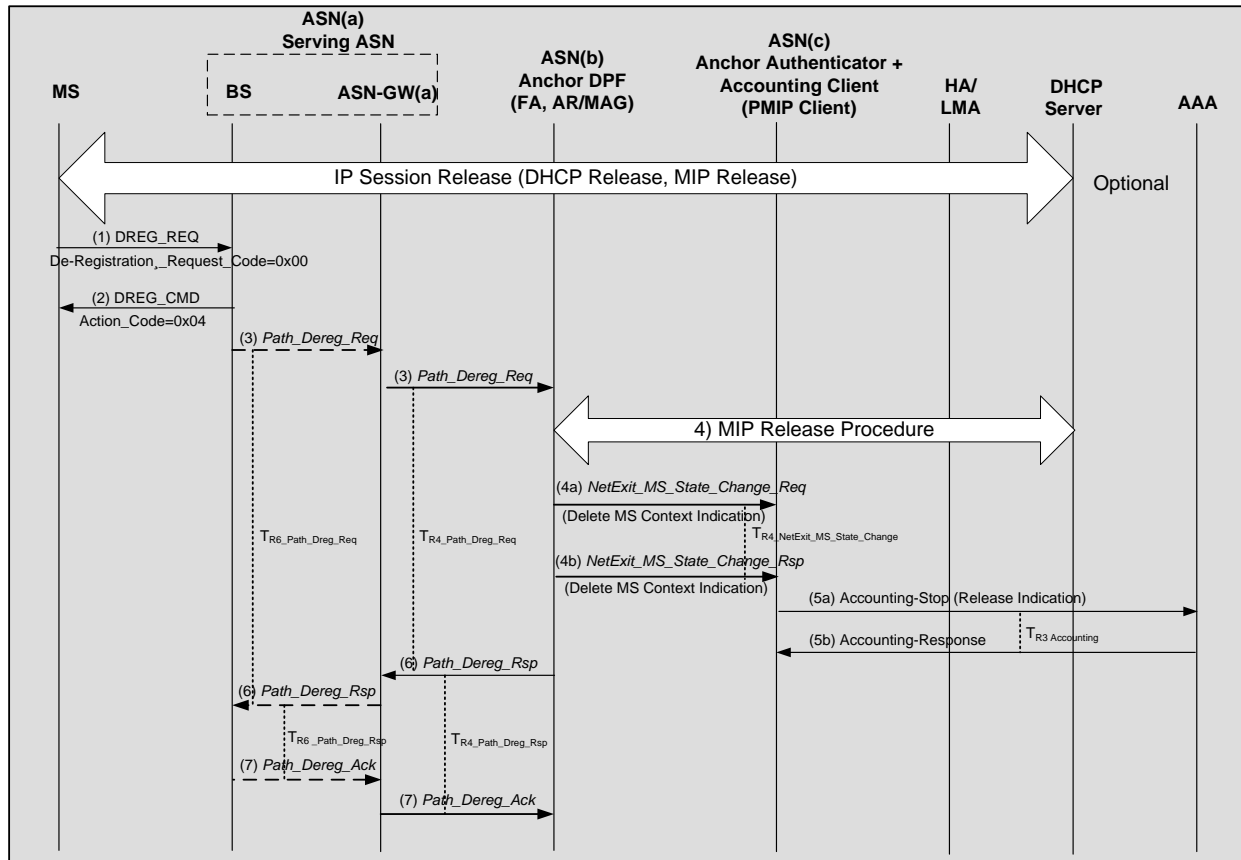


Figure 4-57 – MS Triggered Network Exit (Normal Mode)

##### STEP 1

While the MS has an active session the MS exits the network by sending a DREG\_REQ message to BS in Serving ASN, including De-Registration\_Request Code=0x00.

Before this step, optionally, MS performs initiating DHCP Release Procedure and for a CMIP terminal, MS may perform MIP tunnel release (MIP De-registration) procedure. For the PMIP case, a DHCP Release SHALL trigger the PMIP Client to initiate a MIP tunnel release procedure. For the PMIP6 case using the DHCP Proxy, a DHCPv6 Release (DHCPv4 for an IPv4 managed MS) triggers AR/MAG to initiate release of the MIP transport tunnel established with the LMA.

There may not be DHCP release procedure, i.e., IP is stateless auto-configuration in IPv6, and then the AR/MAG should not initiate a MIP tunnel release at this step.

##### STEP 2

BS sends DREG\_CMD message to the MS including Action Code =0x04.

##### STEP 3

BS sends *Path\_Dereg\_Req* message over R6 to the ASN-GW(a) which in turn SHALL send a *Path\_Dereg\_Req* message over R4 with Power Down Indication to Anchor ASN(b) which contains the Anchor DPF/(FA or AR/MAG).

**STEP 4**

The Anchor ASN(b) associated with the FA/MAG, sends *NetExit\_MS\_State\_Change\_Req* message over R4 to notify ASN(c) (which contains Accounting Client, Anchor Authenticator and PMIP Client) to delete the MS contexts.

Prior to this step, ASN(b) can initiate MIP tunnel release procedure as follows:

For CMIP, if MS did not perform MIP De-registration procedure in the step1, the ASN(b) can perform a MIP De-Registration as specified in [4.8.3.4].

For PMIP, if MS did not perform DHCP Release procedure in the step 1, the *Path\_Dereg\_Req* message over R4 can trigger MIP De-Registration procedure as presented in Section 4.8.2.4.7.

For PMIP6, if there was no DHCPv6/v4 Release in step 1, *Path\_Dereg\_Req* message received over R4 MAY trigger ASN(b) to initiate PMIP6 session release as described in Section 4.8.5.6.

The details regarding MIP session termination are as described in 4.8.

ASN(c) responds to ASN(b) with *NetExit MS State Change\_Rsp* message.

**STEP 5**

ASN(c) containing the Accounting Client sends Accounting Stop message including a Release Indication of MS De-registration to AAA (visited-AAA/Home-AAA) for indicating MS de-registration; AAA server releasing the related MS contexts. In the case of Diameter, ASN(c) also sends a Diameter WSTR command to AAA and AAA responds with a WSTA command following the accounting stop procedure.

**STEP 6**

ASN(b) replies by sending the *Path\_Dereg\_Rsp* over R4 to the Serving ASN(a), which in turns sends a *Path\_Dereg\_Rsp* message over R6 to the BS.

**STEP 7**

The BS sends *Path\_Dereg\_Ack* over R6 to the ASN-GW(a) which in turn will sends a *Path\_Dereg\_Ack* message over R4 to ASN(b). During this procedure, the related entities SHALL release the retained MS context and the assigned a data path resource for the MS.

**4.5.2.1.2 Network Trigger**

The following network entities may initiate MS Network Exit:

- Home AAA server;
- Authenticator/PMIP client;
- Anchor DP/FA, DHCP proxy/relay;
- Serving BS/Serving ASN;
- HA, LMA.

Network Exit may be initiated in situations where Data Path for the MS has already been established or not. Regardless of the data path existence, either Data Path Control (*Path\_Dereg*) or *NetExit\_MS\_State\_Change\_Req/Rsp* messages may be used (means a BS should be able to handle both cases). *NetExit\_MS\_State\_Change\_Req/Rsp* messages MAY be used between any ASN entities. The receiving entity SHALL treat it as a trigger for Network Exit.

When MS Network Exit is signaled not across the data path (i.e., between ASN entities not participating in the data path, e.g., between Anchor DP and Authenticator functional entities), *NetExit\_MS\_State\_Change\_Req/Rsp* messages are used.

#### 4.5.2.1.2.1 AAA Server or Authenticator - initiated MS Network Exit

In this scenario, the triggering of the BS to perform MS deregistration may involve Data Path Control messages (Path\_Dereg) between Anchor DPF and BS as described in the following message flow, or it may be based on *NetExit\_MS\_State\_Change\_Req/Rsp* messages only (see section 4.5.2.1.2.4 as an example of using these messages for triggering the BS).

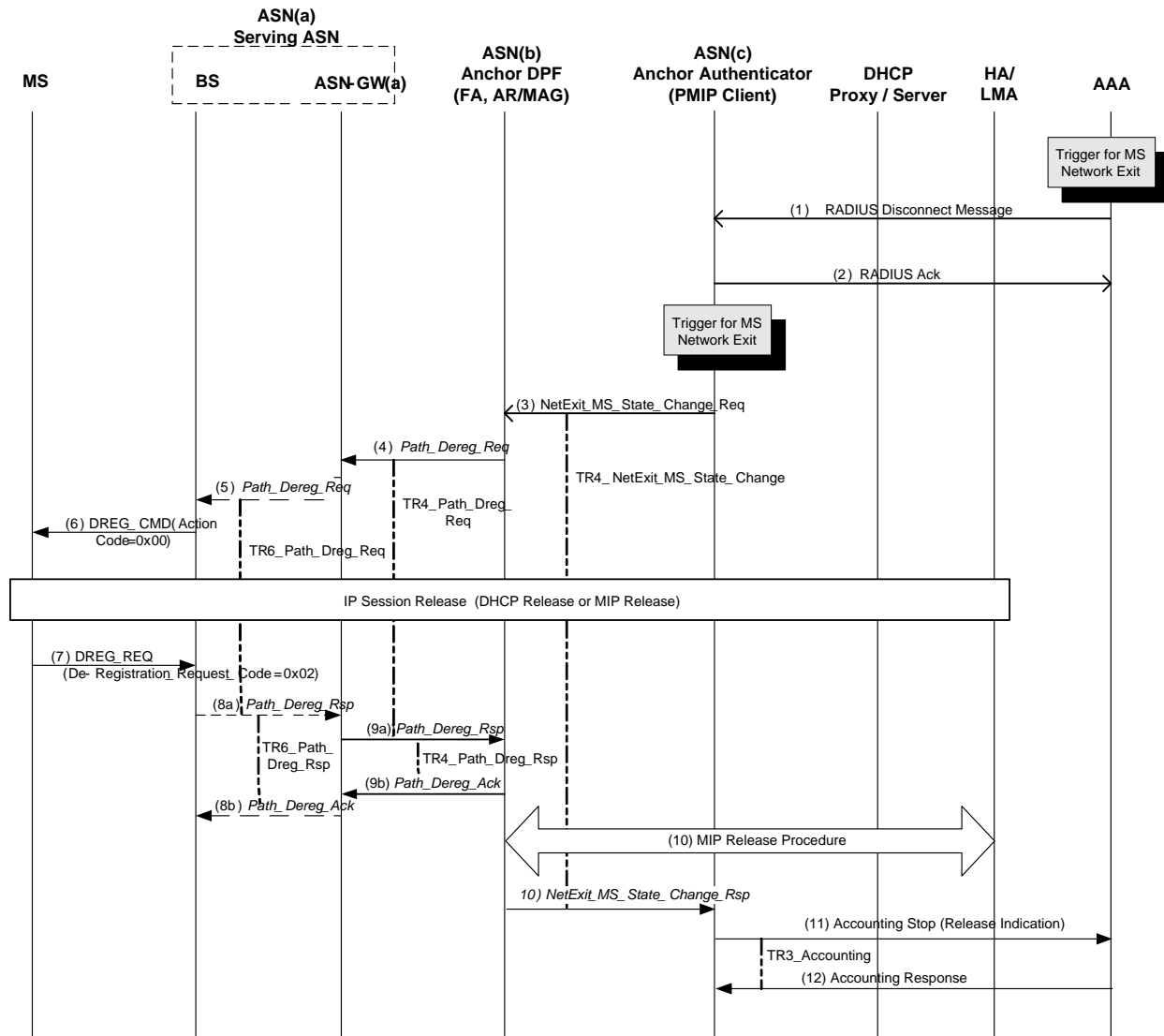


Figure 4-58 – AAA Server/ Authenticator Trigger (Normal Mode)

#### STEP 1

Home-AAA server in the Home CSN takes a decision to deregister the MS based on changing service strategy including user's arrears, report loss of mobile phone by user etc.

The H-AAA sends RADIUS Disconnect message or Diameter WASR command to ASN(c) hosting the Anchor Authenticator (NAS). The message composition is presented in [5.4.1.7].

**STEP 2**

The Anchored Authenticator (NAS) acknowledges RADIUS Disconnect message by sending Disconnect-ACK, and Diameter WASR command by sending a WASA command. The message composition is presented in [5.4.1.7] for RADIUS and in 5.5.1.1.5 for Diameter. If NAS cannot proceed with MS deregistration, it should respond with RADIUS Disconnect-NACK message or Diameter WASA command indicating failure as presented in [5.4.1.6.9] and 5.5.1.1.5.

For Authenticator-initiated MS Network Exit, this trigger occurs locally in the Anchored Authenticator (NAS). This trigger may be caused by graceful shutdown (e.g., PMK lifetime expiry) or some failure situation where MS re-initialization is needed.

**STEP 3**

Authenticator in ASN(c) proceeds with the MS deregistration process by sending a *NetExit\_MS\_State\_Change\_Req* message over R4 to ASN(b) including Action Code TLV set to indicate MS Deregistration from the network.

For PMIP, the ASN(c), which contain PMIP4 client, can perform MIP De-Registration procedure. The details of MIP session termination are covered in the section [4.8].

If the authenticator located in ASN(a), the authenticator can initiate by sending a *NetExit\_MS\_State\_Change\_Req* message to a BS directly including Action Code TLV set to indicate MS Deregistration from the network.

**STEP 4**

ASN(b), which contains Anchor DP/FA functions receives MS Network Exit indication from ASN(c)/Authenticator.

The Anchor DPF initiates data path deregistration procedure toward the Serving BS by sending *Path\_Dereg\_Req* message over R4 to the Serving ASN(a) with Action Code TLV set to indicate MS Deregistration from the network.

**STEP 5**

The Serving ASN(a) forwards *Path\_Dereg\_Req* message over R6 with Action Code TLV to the Serving BS.

**STEP 6**

BS initiates over-the-air MS deregistration process according to the value specified in the Action Code TLV (e.g., by sending DREG-CMD message to MS including R1 Action Code =0x00 to enforce MS network exit). Note that depending on the value of Action Code TLV in *Path\_Dereg\_Req* message, BS should use the corresponding operation over-the-air - DREG-CMD with appropriate Action Code or RES-CMD.

**STEP 7**

MS replies with DREG-REQ message to BS including Deregistration Request Code = 0x02.

Before this step, for CMIP terminal, MS may perform MIP release procedure. For PMIP, MS may perform DHCP release procedure. This DHCP Release triggers PMIP4 client to initiate MIP release procedure. For PMIP6, the MS may perform DHCPv6/v4 Release procedure for its home address.

Note 1: Based on implementation, IP session release may be optional.

Note 2: Based on implementation, this step may be optional. Even if BS does not receive DREG-REQ message from MS, it should be able to detect the completion of over-the-air MS deregistration procedure and then follow the next steps.

**STEP 8**

BS responds to *Path\_Dereg\_Req* message from Serving ASN(a) by *Path\_Dereg\_Rsp* message. This step occurs when BS detects the completion of over-the-air MS deregistration procedure.

Serving ASN(a) acknowledges the receipt of *Path\_Dereg\_Rsp* message by sending *Path\_Dereg\_Ack* message over R6 to the BS.

**STEP 9**

The Serving ASN (a) proceeds with data path deregistration by sending *Path\_Dereg\_Rsp* message over R4 to ASN(b), which contains the Anchor DPF.

ASN(b) acknowledges the receipt of *Path\_Dereg\_Rsp* message by sending *Path\_Dereg\_Ack* message over R4 to ASN(a).

**STEP 10**

ASN(b)/Anchor DPF terminates the data path. For CMIP, if MIP deregistration has not been performed by MIP client as a part of IP Session release step, ASN(b)/FA performs MIP De-Registration as specified in [4.8.3.4].

For PMIP, if MS did not perform DHCP Release procedure in the step 7, the ASN(c) SHALL perform MIP De-Registration.

For PMIP6, if MS did not perform DHCPv6/v4 Release or if MIP De-Registration was not triggered prior, the ASN(b) SHALL perform PMIP6 session release with the LMA as described in Section 4.8.5.6.

ASN(b)/Anchor DPF confirms MS Network Exit to ASN(c)/Authenticator by sending *NetExit\_MS\_State\_Change\_Rsp* message.

**STEP 11**

Accounting Client in the ASN(c) sends Accounting-Request (Stop) message including a release indication to AAA (Visited-AAA/ Home-AAA). In the case of Diameter, ASN(c) also sends a Diameter WSTR command to AAA and AAA responds with a WSTA command following the accounting stop procedure.

**STEP 12**

AAA server responds with Accounting-Response message and releases the related MS contexts.

#### 4.5.2.1.2.2 Anchor DPF - initiated MS Network Exit

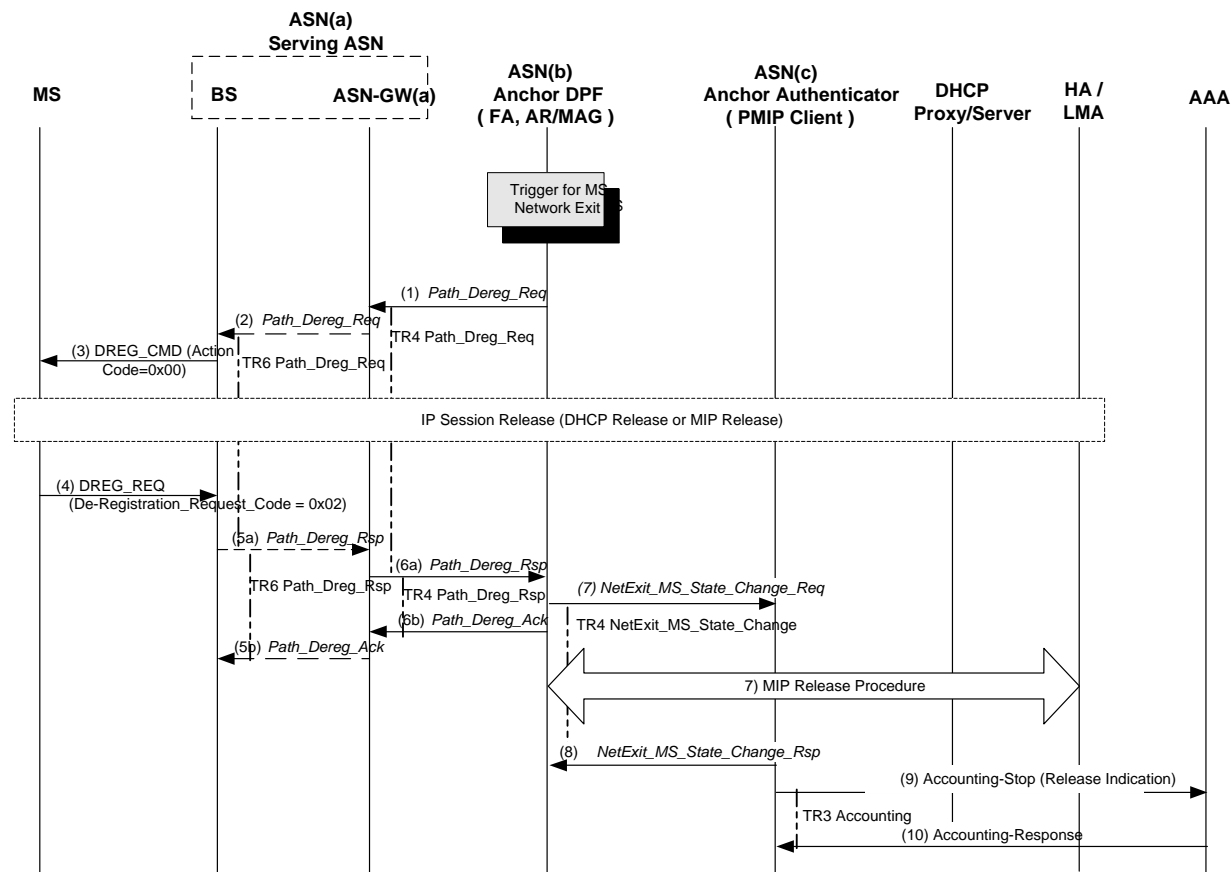


Figure 4-59 – Anchor DPF/FA Trigger (Normal Mode)

#### STEP 1

MS Network Exit trigger occurs in Anchor DPF ASN(b) hosting FA or AR/MAG function. This trigger may be caused by some failure situation where MS re-initialization is needed.

Anchor DPF initiates data path deregistration procedure along the data path by sending *Path\_Dereg\_Req* message over R4 with Action Code TLV set to indicate MS Deregistration from the network.

#### STEP 2 - 6

These steps are similar to steps 5 - 9 of 4.5.2.1.2.1.

#### STEP 7

ASN(b)/ Anchor DPF terminates the data path and signals MS Network Exit to ASN(c)/ Authenticator by sending *NetExit\_MS\_State\_Change\_Req* message over R4 including Network Exit Indicator TLV.

For CMIP, if MIP deregistration has not been performed by MIP client as a part of IP Session release step, ASN(b)/ FA performs MIP De-Registration as specified in [4.8.3.4].

For PMIP6, if MIP De-Registration was not performed as part of IP Session release following step 3, the ASN(b) which hosts the AR/MAG SHALL triggers PMIP6 session release with the LMA as specified in Section 4.8.5.6.

## STEP 8

ASN(c)/ Authenticator receiving *NetExit\_MS\_State\_Change\_Req* message with MS Network Exit indication, responds with *NetExit\_MS\_State\_Change\_Rsp* message.

For PMIP, if MS did not perform DHCP Release procedure in the step 4, the ASN(c), which contain PMIP4 client, SHALL perform MIP De-Registration procedure. The details of MIP session termination are covered in the section 4.8 .

## STEP 9 – 10

These steps are similar to steps 11 – 12 of 4.5.2.1.2.1. In the case of Diameter, ASN(c) also sends a Diameter WSTR command to AAA and AAA responds with a WSTA command following the accounting stop procedure.

### 4.5.2.1.2.3 BS - initiated MS Network Exit

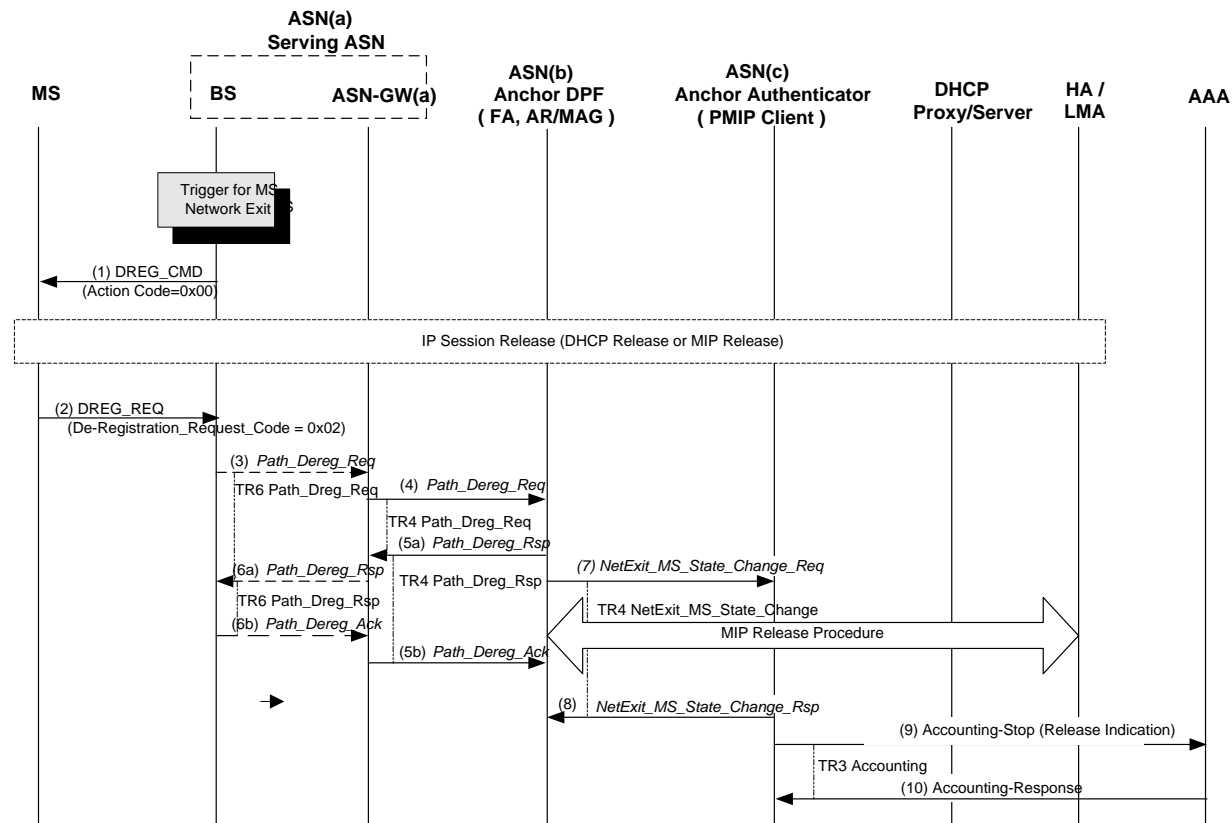


Figure 4-60 – BS Trigger (Normal Mode)

## STEP 1

MS Network Exit trigger occurs in the Serving BS. Generally, BS in the Serving ASN should not be an initiator of MS Deregistration. In the case of failure, it should report the problem to Authenticator and wait for command from ASN entity. If, in this state, failure occurs in communications with ASN entities or there is no command during some timeout, BS may start MS Deregistration process by sending the DREG\_CMD to the MS.

BS sends DREG-CMD message to MS including Action Code =0x00 to enforce MS network exit.

## STEP 2

MS replies with DREG-REQ message to BS including Deregistration Request Code = 0x02.

Before this step, for CMIP terminal, MS may perform MIP release procedure. For PMIP, MS may perform DHCP release procedure. This DHCP Release triggers PMIP4 client to initiate MIP release procedure. For PMIP6, MS may perform DHCPv6/v4 release procedure triggering ASN(b) to initiate PMIP6 release procedure.

Note 1: Based on implementation, IP session release may be optional.

Note 2: Based on implementation, this step may be optional. Even if BS does not receive DREG-REQ message from MS, it should be able to detect the completion of over-the-air MS deregistration procedure and then follow the next steps.

### STEP 3

BS sends *Path\_Dereg\_Req* message with Network Exit Indicator along the data path to Serving ASN(a). This step occurs when BS detects the completion of over-the-air MS deregistration procedure.

### STEP 4

The Serving ASN(a), receiving *Path\_Dereg\_Req* message with Network Exit Indicator, proceeds with data path deregistration by sending *Path\_Dereg\_Req* along the data path to ASN(b)/Anchor DPF over R4.

### STEP 5

ASN(b)/ Anchor DPF, receiving *Path\_Dereg\_Req* message with Network Exit Indicator, responds to ASN(a) with *Path\_Dereg\_Rsp* message.

ASN(a), receiving *Path\_Dereg\_Rsp*, acknowledges it by *Path\_Dereg\_Ack*.

### STEP 6

The Serving ASN(a) sends *Path\_Dereg\_Rsp* message to BS over R6.

BS, receiving *Path\_Dereg\_Rsp*, acknowledges it by *Path\_Dereg\_Ack*.

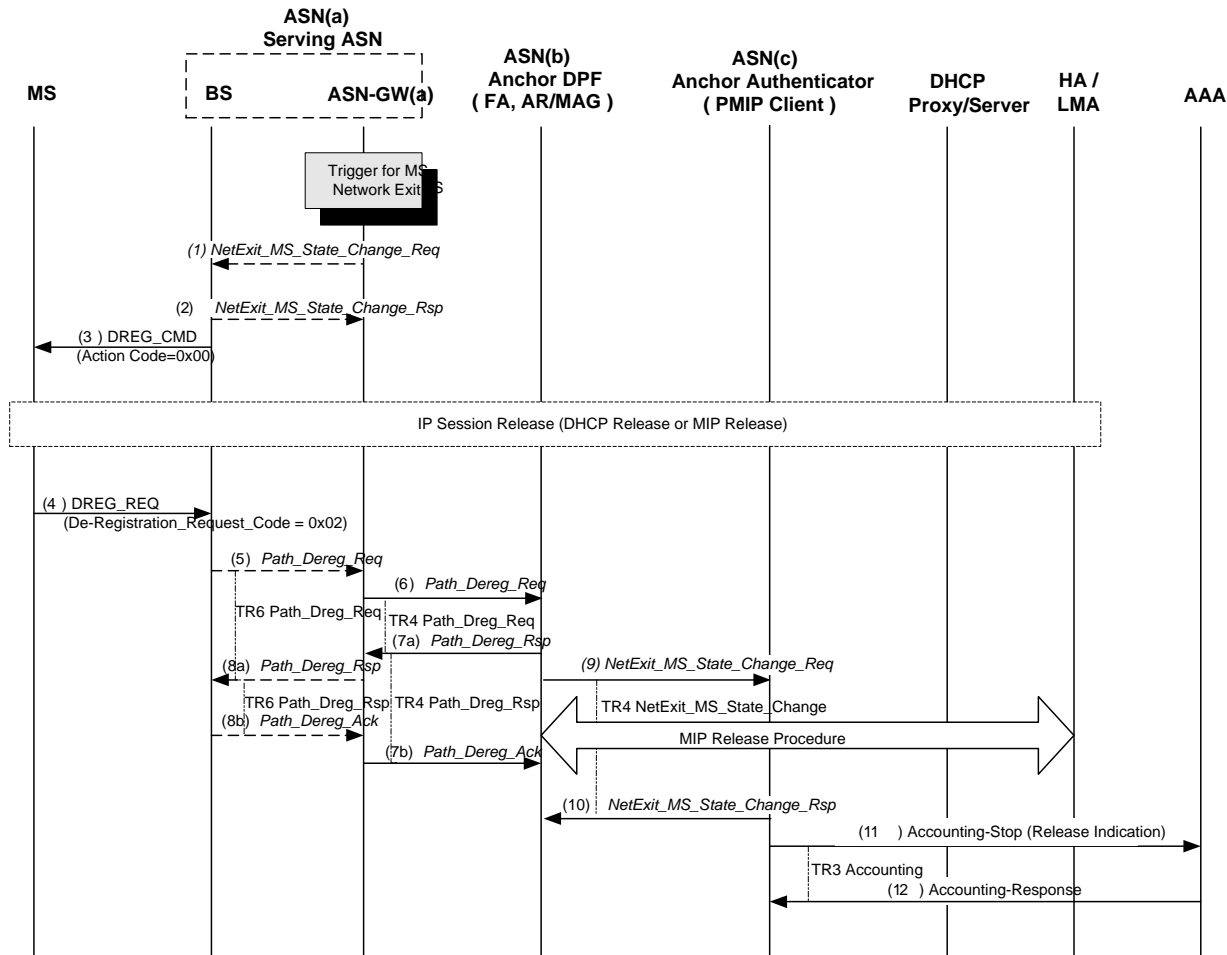
### STEP 7 – 10

These steps are similar to the steps 7 – 10 of 4.5.2.1.2.1. In the case of Diameter, ASN(c) also sends a Diameter WSTR command to AAA and AAA responds with a WSTA command following the accounting stop procedure.

#### 4.5.2.1.2.4 ASN entity instigating MS Network Exit in a BS

As mentioned above, Network Exit initiated by ASN entities may be using *NetExit\_MS\_State\_Change\_Req/Rsp* messages to instigate NetExit procedure from a BS. The example of such flow initiated by ASN GW (a) is presented in this subsection.





**Figure 4-61 – ASN entity instigating Net Exit in a BS**

### STEP 1

MS Network Exit trigger occurs in Serving ASN(a).

ASN GW (a) instigates Network Exit procedure by sending *NetExit\_MS\_State\_Change\_Req* message to the BS with Action Code TLV set to indicate MS Deregistration from the network.

### STEP 2

BS in ASN(a) responds by sending *NetExit\_MS\_State\_Change\_Rsp* message over R6 to the ASN-GW(a).

### STEP 3

BS in ASN(a) initiates over-the-air MS deregistration process according to the value specified in the Action Code TLV (e.g., by sending DREG-CMD message to MS with R1 Action Code =0x00 to enforce MS network exit).

Note that depending on the value of Action Code TLV in *NetExit\_MS\_State\_Change\_Req*, BS should use the corresponding operation over-the-air - DREG-CMD with appropriate Action Code, RES-CMD or RNG-RSP with Ranging Result Code = Abort.

## STEP 4 – 12

These steps are the same as steps 2 – 10 presented in [4.5.2.1.2.3]. In the case of Diameter, ASN(c) also sends a Diameter WSTR command to AAA and AAA responds with a WSTA command following the accounting stop procedure.

### 4.5.2.1.2.5 HA/LMA initiated MS Network Exit

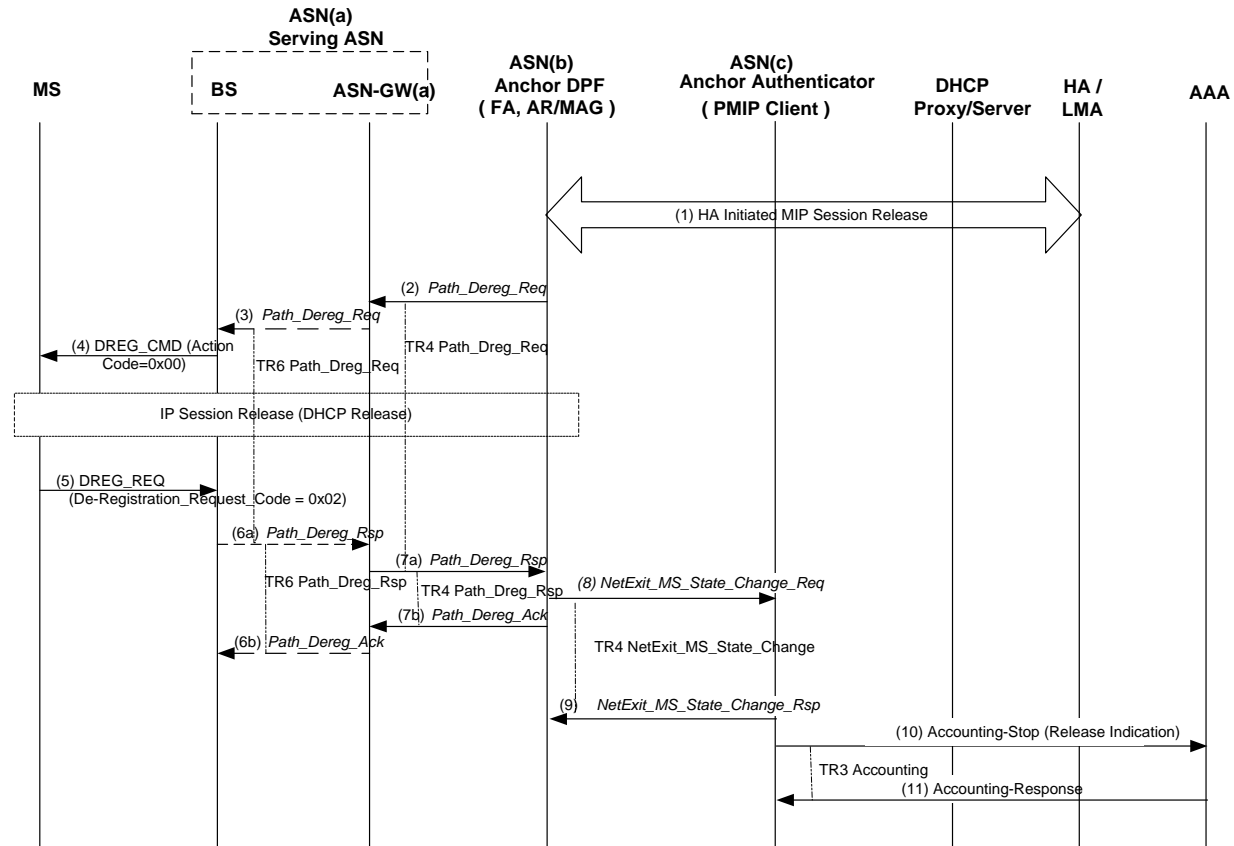


Figure 4-62 – HA initiated MS Network Exit

## STEP 1

HA decides to De-register the MS from the network and performs PMIP Session release for the MS as specified in section 4.8.2.4.7.1.3. For CMIP case the MIP deregistration is performed between the MS, FA and HA. For PMIP6 the LMA initiates Session release by sending the Binding Revocation Indication message as described in Section 4.8.5.6.

## STEP 2 – 4

These steps are the same as steps 1 to 4 in section 4.5.2.1.2.2. The MS unknown about the MIP De-registration for PMIP case, may optionally send DHCPRELEASE. The DHCP Proxy/Relay may silently discard this message.

## STEP 5 – 11

These steps are the same as steps 4 to 10 in section 4.5.2.1.2.2. The Optional procedure for MIP release in step 7 is not performed in this case as it is already done in step 1.

### 4.5.2.2 Idle Mode

In the Idle mode, considering MS exiting network entry, Anchor PC SHALL conduct MS de-registration procedure, and the related network entities SHALL release the resources and delete the MS contexts.

The scenario mainly includes MS power down, resource blocking, fault, or changing service strategy of network side.

#### 4.5.2.2.1 MS Triggered Network Exit (Idle Mode)

There are two options for a MS to trigger network exit while it is in idle mode:

- MS exits idle mode and conducts graceful termination while in active mode. For the network exit procedure, it is covered by Idle exit and Network exit in active mode text.
- Per [11], MS sends RNG\_REQ with power down indication without exiting the idle mode. The following call procedure is for this network exit method.

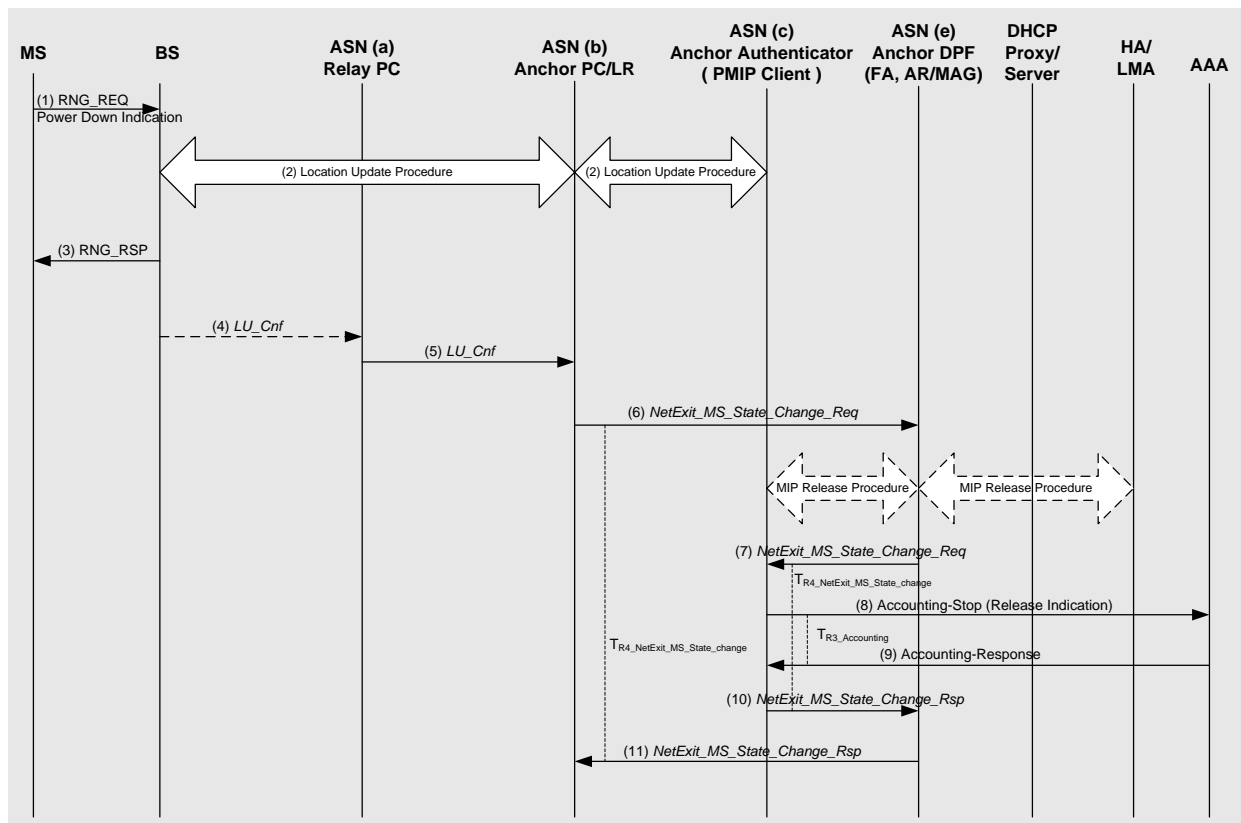


Figure 4-63 – MS Triggered Network Exit (Idle Mode)

## 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 Paging Agent in the BS verifies successfully the RNG\_REQ message based on MS's AK and AK Context, BS/PA and ASN(b) together with Anchor PC SHALL perform a normal location update procedure.

**STEP 3, 4, 5**

The BS replies with RNG\_RSP to the MS and over R6 sends *LU\_Cnf* message including successful indication to the Anchor PC located in ASN(b). Later on Anchor PC/LR in ASN(b) SHALL conduct MS De-registration procedure and the related network entities SHALL release the assigned resource for this MS and delete the MS context.

**STEP 6**

ASN(b)/Anchor PC sends *NetExit\_MS\_State\_Change\_Req* message over R4 including Power Down Indication to ASN(e)/Anchor DPF/FA.

**STEP 7, 10**

ASN(e)/Anchor DPF sends *NetExit\_MS\_State\_Change\_Req* over R4 including delete MS context indication to ASN(c)/Anchor Authenticator.

For PMIP4, CMIP4, and PMIP6 session, before this step, ASN(e)/Anchor DPF SHALL initiate the MIP De-Registration procedure. For PMIP4, ASN(c) containing the Anchor PMIP4 client, ASN(e) containing the FA and the HA can complete a MIP De-Registration procedure based on the normal MIP De-registration procedure. For CMIP, the FA can perform MIP Revocation procedure based on [50]. Additionally the associated entities SHALL release the related MS context and resource retained by these entities. For PMIP6, the AR/MAG can perform MIP Revocation procedure based on [95]. See section 4.8 for details for MIP session termination.

**STEP 8, 9**

ASN(c) that contains the Accounting Client, SHALL send Accounting Stop message including a Release Indication of the MS to the AAA (visited-AAA/Home-AAA) for location update and indication of MS de-registration from the network. The AAA server in turn SHALL release the related MS contexts. In the case of Diameter, ASN(c) also sends a Diameter WSTR command to AAA and AAA responds with a WSTA command following the accounting stop procedure.

**STEP 11**

After releasing the MS context retained by the related entity, the ASN(e) Anchor DPF sends over R4 a NetExit MS State Change Response message to ASN(b)/Anchor PC and the Anchor PC SHALL releases the retained MS context.

**4.5.2.2.2 Network Trigger**

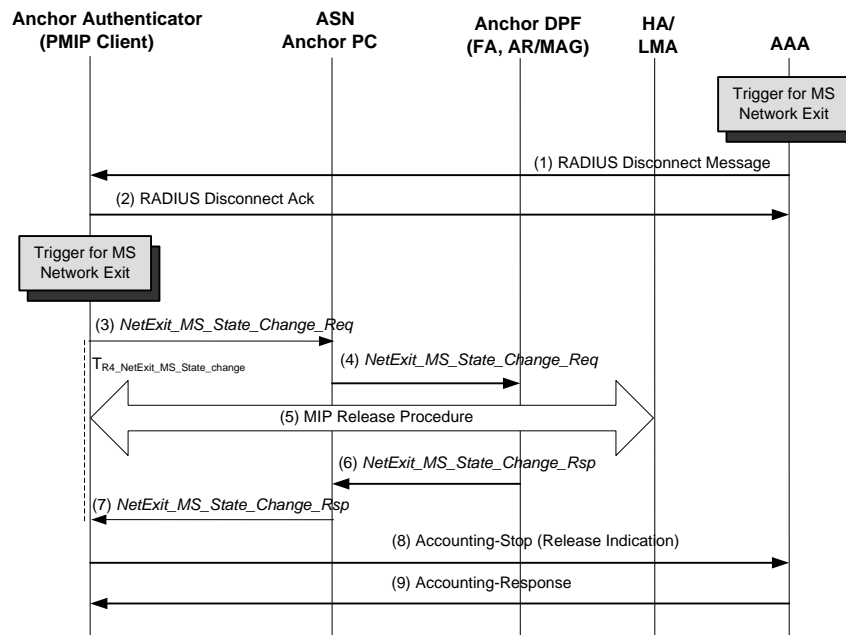
**4.5.2.2.2.1 Ungraceful Network Exit - Network Triggered in Idle Mode**

Even though network MAY awaken the MS and let the MS perform graceful Network Exit Procedure, Network MAY clean up the resources for the given MS. The following network entities can initiate the Network Exit Procedure during idle mode to perform Ungraceful Exit.

- AAA server/Authenticator;
- Paging Controller;
- Anchor DPF with FA or MAG DHCP proxy/relay;
- HA or LMA.

The following subsections describe the cases for Network Exit Procedure in Idle mode.

#### 4.5.2.2.1.1 AAA Server or Authenticator - initiated Network Exit in Idle Mode



**Figure 4-64 – AAA Server/ Authenticator Trigger Ungraceful Network Exit (Idle Mode)**

#### STEP 1

When AAA server decides to disconnect the MS, the AAA MAY initiate the procedure by sending RADIUS Disconnect Message or Diameter WASR command to Authenticator.

#### STEP 2

The Authenticator (NAS) acknowledges RADIUS Disconnect Message by sending Disconnect ACK or Diameter WASR command by sending a WASA command. If NAS cannot proceed with Network Exit procedure, it should respond with RADIUS Disconnect-NACK message or Diameter WASA command indicating the failure.

#### STEP 3

The Anchor Authenticator sends NetExit MS State Change Req including delete MS context indication to Anchor PC.

#### STEP 4

Anchor PC sends NetExit\_MS\_State\_Change\_Req to Anchor DPF with Ungraceful Network Exit Indicator TLV and Delete MS Context Indication TLV so that Anchor DPF can delete the MS related context.

#### STEP 5

The Authenticator triggers the Mobile IP Release procedure.

For PMIP case, the Authenticator ASN, which contains the PMIP4 client, MAY perform MIP De-Registration procedure. The details of MIP session termination are covered in the section [4.8].

For PMIP6 case, the AR/MAG triggers the MIP De-registration as defined in section 4.8.5.6.

# STEP 6

After releasing the MS context the Anchor DPF sends over R4 NetExit MS State Change Rsp message to Anchor PC and the Anchor PC SHALL release the retained MS context.

# STEP 7

The PC deletes all the MS related context and responds the Authenticator by sending NetExit\_MS\_State\_Change\_Rsp.

# STEP 8

Authenticator (NAS) MAY send Accounting-Request (Stop) message including a release indication to AAA.

# STEP 9

AAA server responds with Accounting-Response message and releases the related MS contexts when AAA server receives the Accounting-Request (Stop).

## 4.5.2.2.1.2 Anchor PC - initiated Network Exit in Idle Mode

When the PC decides to perform Network Exit procedure in idle mode, the PC MAY trigger the procedure by sending NetExit\_MS\_State\_Change\_Req. This case MAY happen when the PC failed to page the MS.

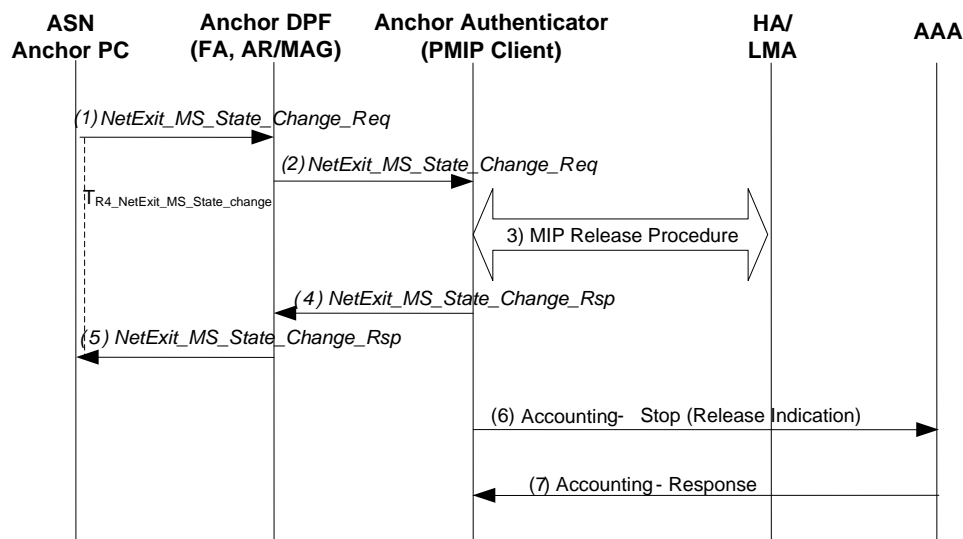


Figure 4-65 – Anchor PC triggered Ungraceful Network Exit (Idle Mode)

# STEP 1

When the Anchor PC decides to perform Network Exit Procedure, it sends NetExit\_MS\_State\_Change\_Req to Anchor DPF with Ungraceful Network Exit Indicator TLV.

# STEP 2

The Anchor DPF sends NetExit MS State Change Req including delete MS context indication to Anchor Authenticator.

# STEP 3

The Authenticator triggers the Mobile IP Release procedure.

For PMIP case, the Authenticator ASN, which contains the PMIP4 client, MAY perform MIP De-Registration procedure. The details of MIP session termination are covered in the section [4.8].

For PMIP6 case, the Authenticator relays the *NetExit\_MS\_State\_Change\_Req* message forward to the Anchor DPF. The AR/MAG that is collocated with the Anchor DPF performs PMIP6 De-Registration procedure as described in section 4.8.5.6. The Anchor DPF responds to Anchor Authenticator with *NetExit\_MS\_State\_Change\_Rsp*.

#### STEP 4

The Authenticator responds the Anchor DPF by sending *NetExit\_MS\_State\_Change\_Rsp*.

#### STEP 5

After releasing the MS context the Anchor DPF sends over R4 *NetExit MS State Change Rsp* message to Anchor PC and the Anchor PC SHALL release the retained MS context.

#### STEP 6

Authenticator (NAS) MAY send Accounting-Request (Stop) message including a release indication to AAA.

#### STEP 7

AAA server responds with Accounting-Response message and releases the related MS contexts when AAA server receives the Accounting-Request (Stop). In the case of Diameter, NAS also sends a Diameter WSTR command to AAA and AAA responds with a WSTA command following the accounting stop procedure.

#### 4.5.2.2.1.3 Anchor DPF - initiated Network Exit in Idle Mode

MIP release procedure (STEP 5) explained below is skipped if Anchor DPF, containing FA or MAG decides to perform Network Exit Procedure based on HA initiated MIP release.

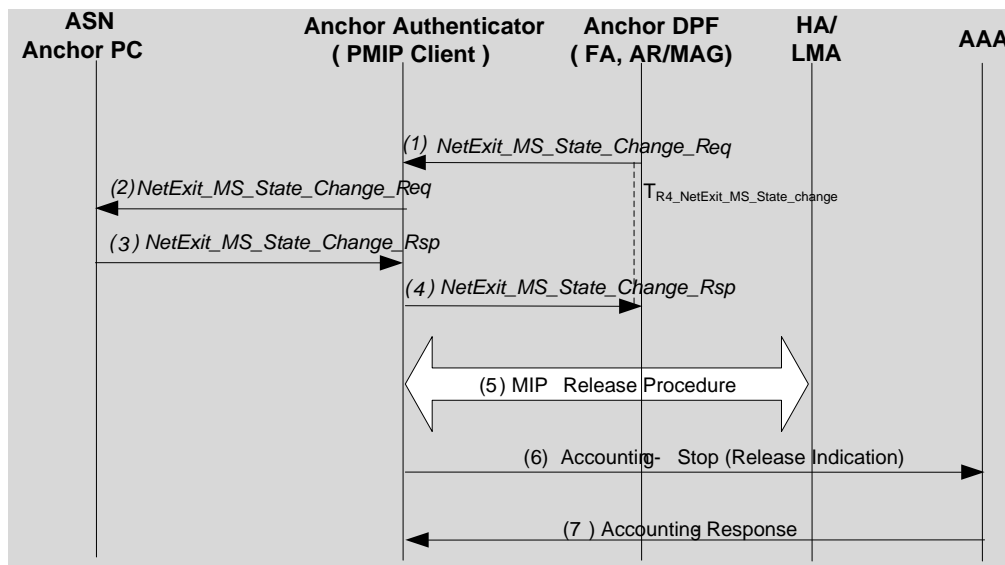


Figure 4-66 – Anchor DPF/FA triggered Ungraceful Network Exit (Idle Mode)

#### STEP 1

When the Anchor DPF containing FA or AR/MAG function decides to perform Network Exit Procedure for the MS in Idle Mode, it sends *NetExit\_MS\_State\_Change\_Req* to the Authenticator with Ungraceful Network Exit Indicator TLV.

**STEP 2**

The Anchor Authenticator sends NetExit\_MS\_State\_Change\_Req to Anchor PC to indicate Ungraceful Network Exit for the MS.

**STEP 3**

The PC deletes all the MS related context and responds the Authenticator by sending NetExit\_MS\_State\_Change\_Rsp.

**STEP 4**

Authenticator sends NetExit\_MS\_State\_Change\_Rsp to the Anchor DPF.

**STEP 5**

If MIP tunnel is present, then Mobile IP Release procedure is triggered.

For PMIP case, the Authenticator ASN, which contains the PMIP4 client, MAY perform MIP De-Registration procedure. The details of MIP session termination are covered in the section [4.8].

For PMIP6 case, the AR/MAG triggers the MIP De-registration as defined in section 4.8.5.6.

**STEP 6 – 7**

These steps are same as the steps 4 to 5 in section 4.5.2.2.1.2. In the case of Diameter, Anchor Authenticator also sends a Diameter WSTR command to AAA and AAA responds with a WSTA command following the accounting stop procedure.

**4.5.2.3 Message Composition**

**4.5.2.3.1 R4/ R6 Data Path Control Messages**

MS Network Exit may be indicated using Path De-Registration message exchange.

The *Path\_Dereg\_Req* message composition is shown in Table 4-51:

**Table 4-51 – 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	M	
>BS ID	5.3.2.25	M	
MS Info	5.3.2.103	M	Compound TLV including information about MS.
>Anchor ASN 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.
>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.



IE	Reference	M/O	Notes
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.
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.).

#### 4.5.2.3.2 R4/R6 MS State Change Messages

*NetExit\_Ms\_State\_Change\_Req* message is used to indicate or command MS Network Exit. The message composition is presented in Table 4-52:

**Table 4-52 – NetExit MS State Change Req Message Composition**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	O	Unique MS R6 context identifier. SHALL be present if an R6_Context_ID has been assigned to the MS at the time of initial network entry.
BS Info	5.3.2.26	M	Compound TLV including information about BS.
>BS ID	5.3.2.25	M	Unique BS Identifier.
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.).
Ungraceful Network Exit Indicator	5.3.2.274	O <sup>4</sup>	If present, indicates the reason of ungraceful network exit (e.g., Ungraceful Network Exit No Reason, AAA initiated Ungraceful Network Exit, etc.).
Delete MS Context Indication	5.3.2.366	O	If presented, indicates the release of the MS context.
MS Info	5.3.2.103	O	Compound TLV including information about MS.

<sup>4</sup> “Ungraceful Network Exit Indication” TLV is presented for network triggered ungraceful network exit in idle mode.

IE	Reference	M/O	Notes
>Anchor ASN 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.

*NetExit MS State Change\_Rsp* message is sent in response to *NetExit\_MS State Change\_Req* message. This message composition is presented in the Table 4-53:

**Table 4-53 – NetExit MS State Change\_Rsp Message Composition**

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	O	Unique MS R6 context identifier. SHALL be present if an R6_Context_ID has been assigned to the MS at the time of initial network entry.
Failure Indication	5.3.2.69	O	Indicates the reason of failure.
Delete MS Context Indication	5.3.2.366	O	If presented, indicates the release of the MS context.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

#### 4.5.2.3.3 R3 AAA Messages

Home-AAA server MAY trigger MS Network Exit process using RADIUS and Diameter procedure:

- RADIUS Disconnect-Request message or Diameter WASR command is sent by AAA to NAS to initiate MS Network Exit;
- RADIUS Disconnect-ACK message or Diameter WASA command is sent by NAS to AAA as a positive response to the request;
- RADIUS Disconnect-NACK message or Diameter WASA command indicating failure is sent by NAS to AAA as a negative response to the request (e.g., MS context is not found).

The message composition is presented in 5.4.1.7 and 5.5.1.1.5:

#### 4.5.2.4 Network Exiting Timers and Considerations

The following Timers are used to support Network Exiting procedures.

$T_{R6\_Path\_Dreg\_Req}$ : This Timer is started by the BS upon transmission of *Path\_Dreg\_Req* and stopped upon the reception of the *Path\_Dreg\_Rsp*.

$T_{R4\_Path\_Dreg\_Req}$ : This Timer is started by ASN-GW(a) upon transmission of *Path\_Dreg\_Req* to ASN(b) Anchor DPF and stopped upon the reception of the *Path\_Dreg\_Rsp*.

$T_{R4\_NetExit\_MS\_State\_change}$ : This Timer is started by ASN(b) Anchor DPF upon transmission of *NetExit\_MS State Change\_Req* message to ASN(c) (which contains Accounting Client, Anchor Authenticator and PMIP Client) and stopped upon reception of *NetExit\_MS State Change\_Rsp*.

$T_{R3\_Accounting}$ : This Timer is started by ASN(c) after transmission of *Accounting-Stop* message to the AAA and stopped upon reception of *Accounting-Response*.

$T_{R6\_Path\_Dreg\_Rsp}$ : This Timer is started by ASN-GW(a) upon transmission of *Path\_Dreg\_Rsp* and stopped upon reception of *Path\_Dreg\_Ack*.

$T_{R4\_Path\_Dreg\_Rsp}$ : This Timer is started by ASN(b) Anchor DPF upon transmission of *Path\_Dreg\_Rsp* and stopped upon reception of *Path\_Dreg\_Ack*.

Table 4-54 - shows the default value of timers and also indicates the range of the recommended duration of these timers. Note that these values are provisioned in Release 1.5.

**Table 4-54 – Network Exit Timer Values for R4 and R6**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
$T_{R6\_Path\_Dreg\_Req}$	TBD		TBD
$T_{R4\_Path\_Dreg\_Req}$	TBD		TBD
$T_{R4\_NetExit\_MS\_State\_Change}$	TBD		TBD
$T_{R3\_Accounting}$	TBD		TBD
$T_{R6\_Path\_Dreg\_Rsp}$	TBD		TBD
$T_{R4\_Path\_Dreg\_Rsp}$	TBD		TBD

#### 4.5.2.4.1 Timer Expiry

Table 4-55 shows the details of the corresponding action(s) associated with timer expiry. Upon each timer expiry, if maximum retries has not exceeded, the related message is retransmitted and timer is restarted. Otherwise corresponding action(s) should be performed as indicated in Table 4-55.

**Table 4-55 – Actions after Timer Max Retry**

Timer	Entity where Timer Started	Action(s)
$T_{R6\_Path\_Dreg\_Req}$	BS	The Network Exit procedure continues
$T_{R4\_Path\_Dreg\_Req}$	ASN-GW(a)	The Network Exit procedure continues
$T_{R4\_NetExit\_MS\_State\_Change}$	ASN(b) Anchor DPF	The Network Exit procedure continues
$T_{R3\_Accounting}$	ASN(c) (which contains Accounting Client).	The Network Exit procedure continues
$T_{R6\_Path\_Dreg\_Rsp}$	ASN-GW(a)	The Network Exit procedure continues
$T_{R4\_Path\_Dreg\_Rsp}$	ASN(b) Anchor DPF	The Network Exit procedure continues

## 4.6 QoS and SFID Management

### 4.6.1 Introduction

This section describes the control protocol and messaging to realize the QoS-related functions described in section 7.6 of the NWG Stage 2 specification [1]. The control protocol is based on RADIUS or Diameter and transported over the ASN transport protocol specified in section 4.

This specification defines the following procedures:

- Pre-provisioned service flow creation, modification, and deletion.
- Initial Service Flow creation, modification and deletion.

- c. Dynamic Service Flow creation, modification and deletion
- d. Static QoS policy provisioning between AAA and Anchor-SFA.
- e. Service Flow ID management.
- f. Modification of existing ISF and pre-provisioned SFs based on updated QoS profiles from the AAA.

## 4.6.2 Functional Model

The QoS functional model is illustrated in chapter 7.6.2 “QoS Functional Elements” of [1]. This model indicates entities including the AAA, the PCRF, the A-PCEF, the Anchor-SFA, Serving-SFA and the SFM, and peering relationships between the AAA and the SFA, and the SFA and the SFM. Relationship between PCRF and PCEF is specified in [3]. In addition, there is a peering 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.

PCC based QoS control by PCRF and PCEF is not covered in this section and is described in [3].

### 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 AAA messages to the HAAA. For each subscriber, the QoS profile includes 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 RADIUS Access-Request packet or Diameter WDER command. Further, HAAA may update the provided QoS profile while a subscriber is attached to the network (i.e., during an ongoing WiMAX session).

One Subscriber QoS profile and associated policy may be identified by a set of ServiceProfileIDs if they are pre-provisioned in ASN. When a ServiceProfileID is used, HAAA maps Subscriber QoS profile (for example, premium, gold, silver and bronze level per-subscriber profile) into one or more ServiceProfileIDs.

## 4.6.4 Service Flow Management

QoS-related messages as defined in section 4.6.5 are used to create, modify and delete service flows over the air. NWG stage-2 specification [1] (section 7.6.3) defines following:

- Pre-provisioned service flow creation, modification and deletion;
- Dynamic service flow creation, modification and deletion
- Initial Service Flow creation and deletion;
- Service Flow management to support MS mobility;

#### 4.6.4.1 Pre-Provisioned Service Flows

Pre-provisioned service flows are service flows with the authorization to be activated and deactivated at any time while a subscriber is attached to a network. They are provided to the MS at network entry after successful MS access authentication. Service flows which are marked with the “Active” flag SHALL be activated at the same time. In case of a QoS profile update triggered by the HAAA, the Anchor-SFA SHALL update the service flows accordingly as soon as possible.

Figure 4-72 describes protocol actions allowing pre-provisioned service flow setup. If any of the pre-provisioned service flows other than the initial service flow of the corresponding CS type (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 of the corresponding CS type for the associated MS is set, the MS SHALL be denied of the service by the local ASN of the corresponding CS type.

There may be a need to create a Service Flow with “wildcard classifier”, allowing any packet of the corresponding CS type to be classified/ transferred over the Service Flow. In this case, “wildcard classifier” MUST be formatted as a Packet Classification Rule compound TLV including Classification Rule Index TLV and excluding all the TLVs specific for classification / matching criteria’s (such as e.g., IP TOS/DSCP Range and Mask TLV, Protocol TLV, IP Source Address and Mask TLV, etc.). For Ethernet CS service flow, the ethernet related information should be included in the Packet Classification Rule TLV for classification/matching criteria, such as the MAC source address, MAC destination address, ethernet type, User Priority Range, SVLAN ID, CVLAN ID.

##### 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 RADIUS Access-Accept packet or Diameter WDEA command from AAA server. The AAA server SHALL include the QoS profile in that message (section 5.4.1.1) sent to AAA-client. This information is provided to the Anchor-SFA. The 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.

QoS profile might also be updated with a Change-of-Authorization by the HAAA which may require new service flows. In such a case, the Anchor-SFA SHALL trigger the creation of the service flows accordingly as soon as possible.

##### 4.6.4.1.2 Delete Service Flow

Deletion of service flows may take place during an explicit trigger by the Anchor-SFA, as part of the network exit procedure (as described in section 4.5) or in case of error handling. Explicit triggers to delete service flows are not supported.

QoS profile might also be updated with a Change-of-Authorization by the HAAA which may require deletion of existing service flows. In such a case, the Anchor-SFA SHALL trigger deletion of the service flows accordingly as soon as possible.

##### 4.6.4.1.3 Modify Service Flow

Because of a QoS profile update triggered by the HAAA, Anchor-SFA might decide to update existing service flows. In such a case, the Anchor-SFA SHALL trigger the update of the service flows as soon as possible.

#### 4.6.4.2 Initial Service Flow

The Initial Service Flow is a special kind of a Pre-Provisioned Service Flow as described at the previous section. Among the set of pre-provisioned unicast service flows, the very first pair of service flows (i.e., for uplink and downlink) that are initiated by the SFA are called the Initial Service Flows (ISF). For each CS type that is required by the MS, a separate pair of ISFs is required.

The purpose of the ISF is that it is used by the MS and the ASN to transfer delay tolerant control traffic such as standards-based IP configuration management and IP client application signaling (e.g., DHCP DISCOVERY, FA Advertisement, Mobile IP Registration, Router Advertisement, SIP signaling etc.) in case of IP-CS as well as configuration management signaling required for Ethernet in case of ETH-CS.

1 If any of the initial service flows of a given CS type for the associated MS is failed to be activated by the local ASN,  
2 the MS SHALL be denied of the service for the given CS type. If none of the CS types can be activated successfully  
3 for the MS, the MS SHALL be denied of the service by the local ASN. Otherwise, if at least one of the CS types of  
4 the MS is operational, the ASN SHALL continue the support the MS operation at the local ASN.

5 The number of retries for the local ASN to attempt to establish the ISFs for the given CS type is local network  
6 policy decision and is outside the scope of this specification.

#### 7 **4.6.4.2.1 IP-CS Related Issues**

8 Since the ISF is established prior to the IP address assignment to the MS, the ASN cannot rely on the IP header  
9 information initially to determine the proper routing decision to forward any downlink traffic destined to the MS.  
10 Therefore, a special context binding, which contains the MSID and/or MS's NAI information, is required to be  
11 installed at the ASN to associate with the peer SFIDs of the ISF (i.e., the two unidirectional SFIDs for uplink and  
12 downlink) for the given MS to process the uplink and downlink IP packets. In the case when multiple pre-  
13 provisioning service flows including the ISF are established before the IP address assignment to the MS, for the IP  
14 CS based ISF, the special context binding may have to be done at the service flow level in order to allow the  
15 downlink IP client application signaling packet to be directed to the appropriate ISF transport over R6. During the  
16 time of initial creation of ISF to IP address acquisition is complete, all other pre-provision service flows SHALL not  
17 transport any IP traffic. The existence of the ISF does not preclude the MS to send IP configuration and IP client  
18 application signaling over another service flow that has been created by the MS once the MS has been assigned with  
19 an IP address with the support of ISF. Except from the time of creation, an ISF is treated like any other pre-  
20 provisioned service flow (like from the parameters settings as well as from the accounting perspective). Once the  
21 ASN is aware of the assigned IP address for the MS, ASN MAY perform the following steps:

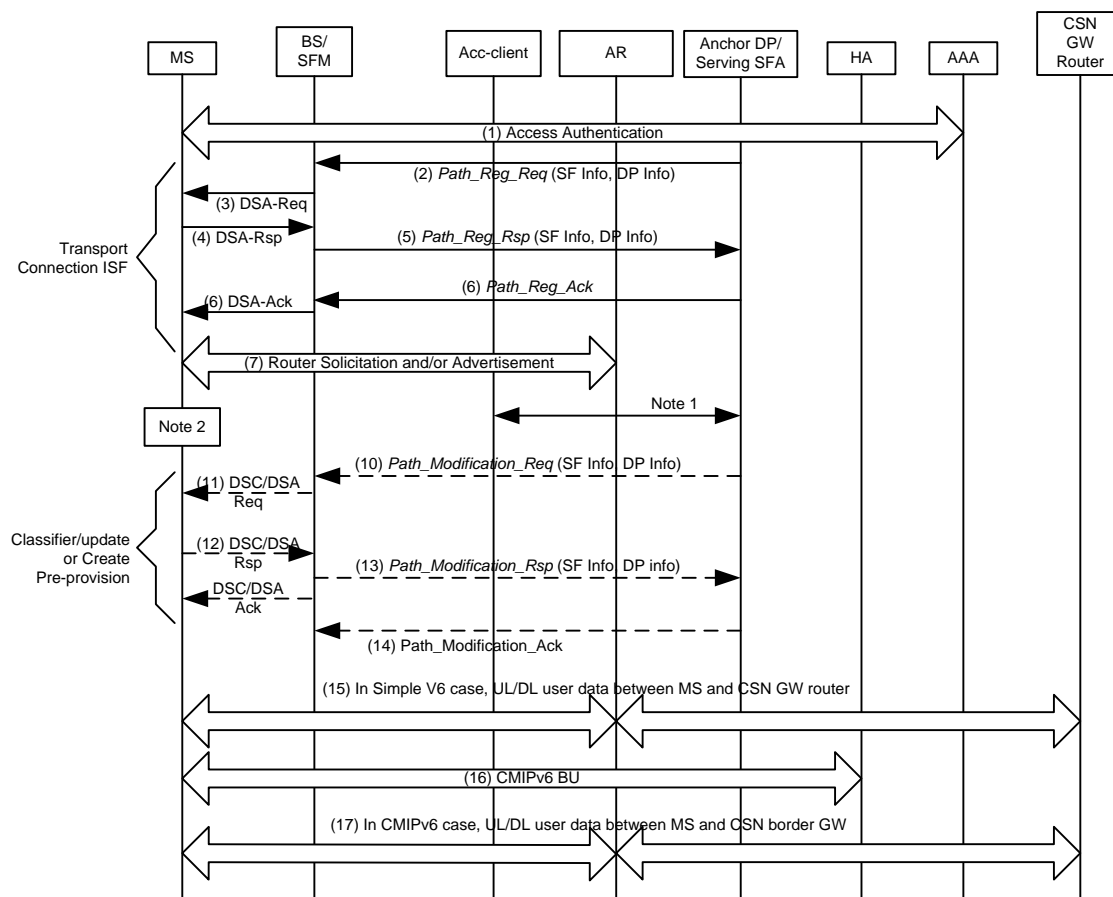
- 22 • Update the classifier and QoS policy of the ISF, and any existing pre-provisioned service flow, which are  
23 created during the ISF.

24 In the case where ISF was created and pre-provisioned flow was not created, ASN SHALL initiate the service flow  
25 creation request and apply the QoS policy to the pre-provisioned service flow.

26 Section 4.8, CSN Mobility Management supports four different IP address assignment mechanisms for the MS.

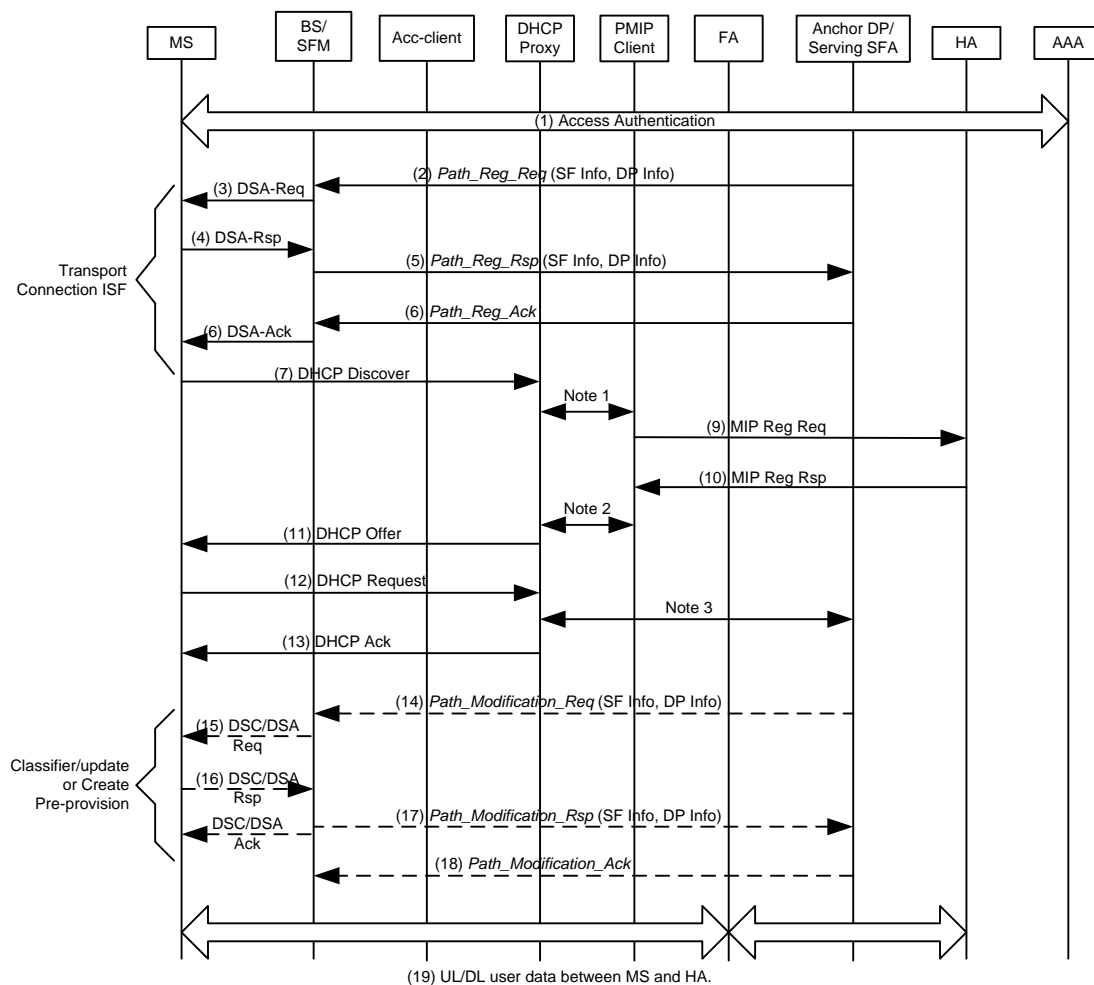
27 Figure 4-67, Figure 4-68, Figure 4-69 and Figure 4-70 show trigger and steps for updating the ISF and any existing  
28 pre-provision service flow for Simple IPv6/CMIP6, PMIP4, CMIP4 and for PMIP6 services in the respective order.

29 The purpose of the figures in this section is to contextualize the ISF data path setup with classifiers. The figures are  
30 informative. For further details, refer to the specific sections in this document.



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.

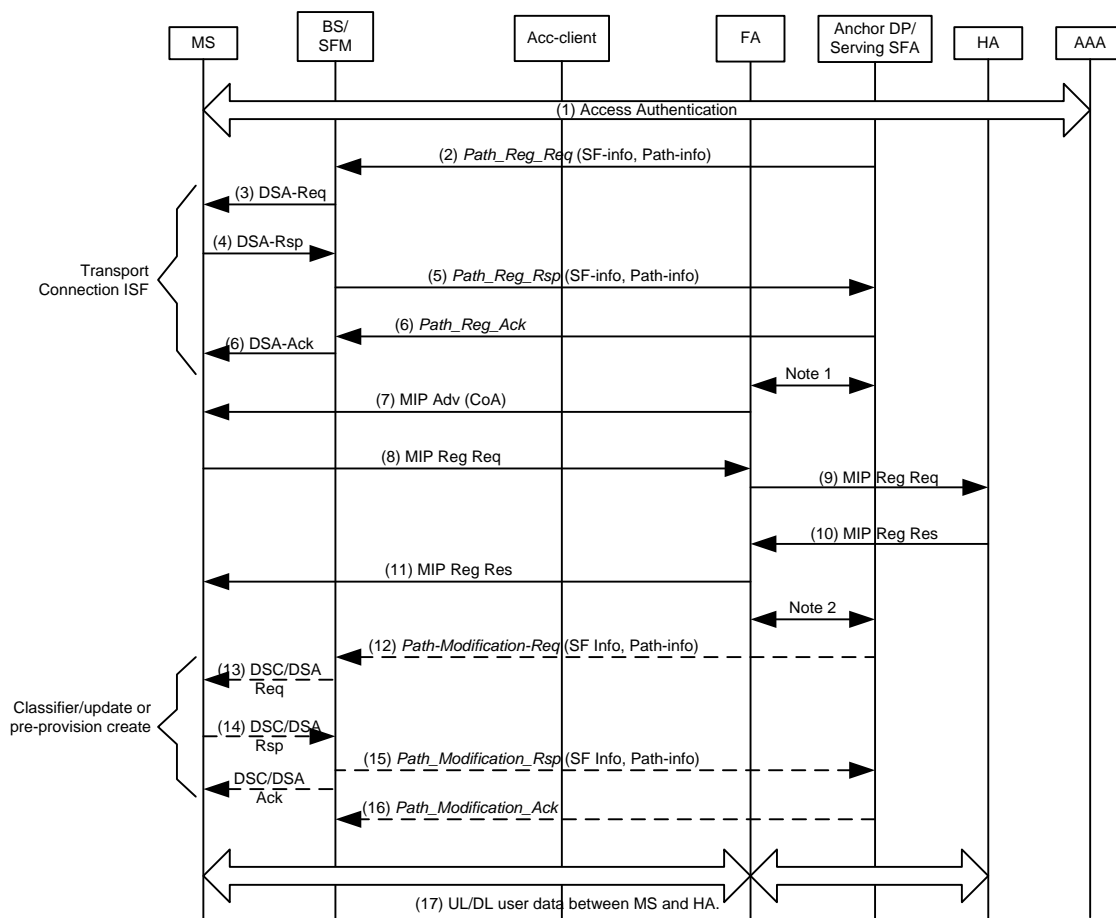
**Figure 4-67 – ISF Classifier Update for IPv6**



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).

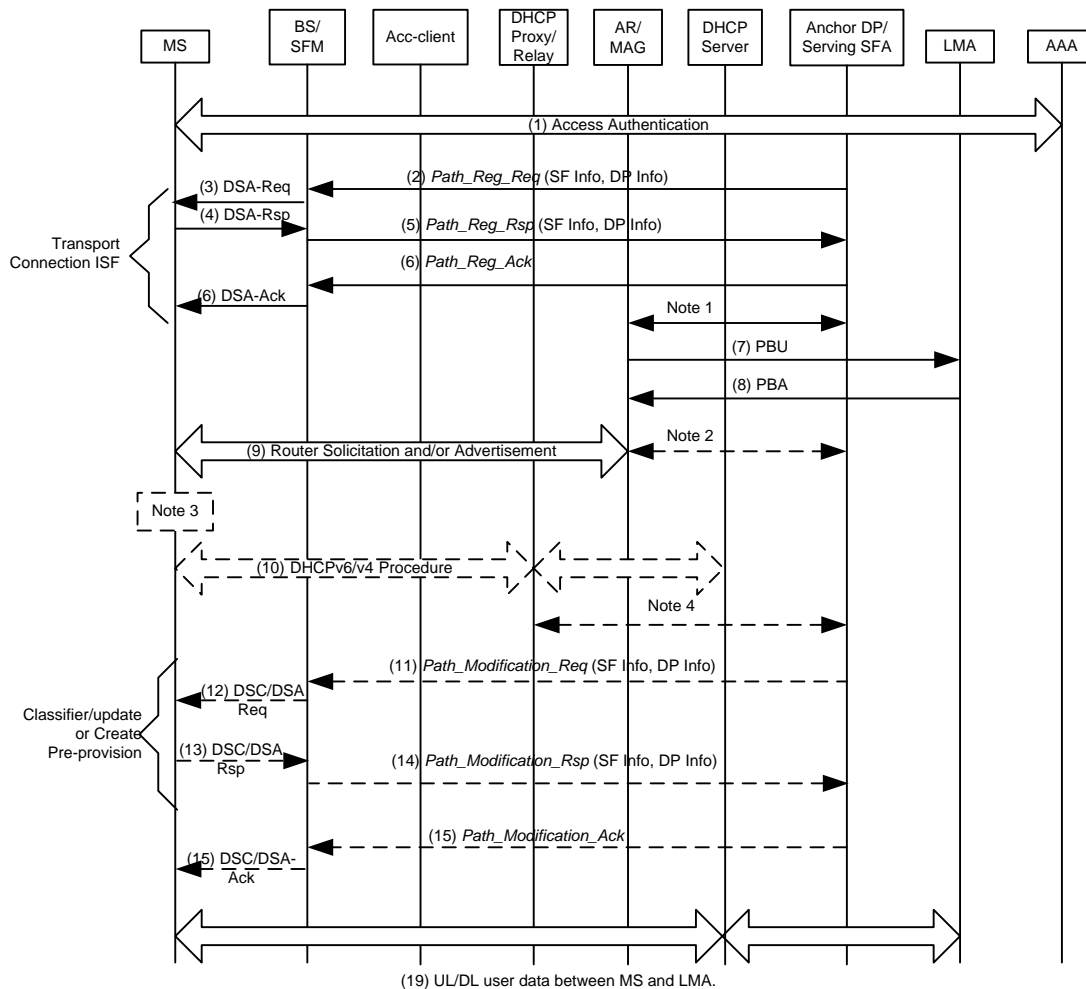
**Figure 4-68 – ISF Classifier Update for PMIP4**





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).

**Figure 4-69 – ISF Classifier Update for CMIP4**



Note 1: AR/MAG may trigger proxy binding update procedure based on network decision to authorize PMIPv6 service.  
Note 2: (For IPv6 MS) In the case the local policy for IPv6 configuration is address auto-configuration, AR/MAG triggers the Anchor DP/Serving SFA to update the SF classifier (out of scope).  
Note 3: In the case that Managed Flag is set to zero in the Router Advertisement message, MS auto-configures the IPv6 address and may proceed with DAD. Otherwise, MS triggers the DHCPv6 procedure. An IPv4 MS always initiates DHCPv4.  
Note 4: DHCP Client in the ASN triggers the Anchor DP/Serving SFA to update the SF classifier (out of scope).

**Figure 4-70 – ISF Classifier Update for PMIPv6**

#### 4.6.4.2.2 Ethernet-CS Related Information

For ETH-CS, an Ethernet specific ISF SHALL be established when the authentication procedure is completed successfully or because of a QoS-profile modification triggered by the HAAA. This ISF SHALL be used for any initial traffic specific for the protocol defined by the Ethernet Type. For IPoETH-CS, the Ethernet specific ISF SHALL be used in the same way as the IP-CS specific ISF (see 4.6.4.2.1).

In the case of ETH CS, the QoS profile of a service flow MAY contain additional information for the processing of VLAN tags. The supported functions for processing of the VLAN tags are specified in chapter 7.6.8 and 7.6.9 in the Stage 2 document. The TLVs for VLAN tag processing are defined in chapter 5 of this document.

#### 4.6.4.2.3 Common Issues

At the ASN, the SFA is responsible for assigning SFID to the service flow. As the pre-provisioning service flow information including the Packet Data Flow ID (PDFID) is downloaded to the ASN after the successful MS access authentication, the SFA is responsible to map one or more PDFIDs to a set of unidirectional service flows dependent on the service flow policy configuration information. Note that the PDFID can represent a unidirectional flow.

To allow an option of the special monitoring of the ISF which is created for different CS types, this specification recommends the first 20 PDFID(s) from the unicast group of PDFIDs to be assigned to the ISF (i.e., 1 – 20 ) in both the uplink and downlink directions for each MS – i.e., the service flow pair for the given ISF will be assigned with a PDFID in the uplink , downlink or both directions.

By default, the ISF is assigned with the following set of policies; however, the default local policies can be modified dependent on the MS's subscription profile that is downloaded from the H-AAA or V-AAA after the successful MS access authentication as well as dependent on the local BS's policy.

- Best effort service class;
- Wildcard classifier;
- Transport both IP/Ethernet control and user traffic;
- Per service flow level of the granularity;
- HARQ disabled and ARQ enabled;
- Paging preference is set to 1;
- Traffic indication is set to 1.

To ensure the deterministic connection status of the ISF that the WiMAX application can rely on to leverage the ISF as the IP/Ethernet based management connection, the ISF SHALL remain operational as long as the MS is attached to the ASN. However, if any of the ISFs fails to be supported by the local ASN, the MS SHALL be denied of the service by the local ASN. Similar to other service flows maintenance in the ASN, the SFA is responsible for maintaining the ISF.

#### 4.6.4.2.4 Create Service Flow

An ISF SHALL set the Active flag to guarantee that its creation takes place as part of the network entry procedure where the creation will be triggered by the ASN. It SHALL be guaranteed by the ASN that the Initial Service Flow (ISF) is the first flow of the pre-provisioned service flows to be activated. ISF creation might also take place in case of QoS-profile update triggered by the HAAA. In such a case, the Anchor-SFA SHALL activate the service flow accordingly as soon as possible after the QoS profile update.

#### 4.6.4.2.5 Delete Service Flow

Deletion of service flows can take place as part of the network exit procedure. Also, the ISF SHALL be the last to be deleted when the MS is de-registered its service from the ASN. Deletion of an ISF might also take place in case of QoS-profile update triggered by the HAAA. In such a case, the Anchor-SFA should delete the service flow accordingly as soon as possible. Explicit triggers other than the Network Exit Procedure to delete initial service flows are not supported.

#### 4.6.4.2.6 Modify Service Flow

A modification of the ISF may be necessary if an ASN creates its own ISF which need to be adapted according to the QoS profile received from the home CSN after the allocation of an IP-address. The modification may be prevented if an ASN uses the ISF parameters provided by the CSN at the initial initiation as far as it contains no classifier referencing the IP address of the MS.

Further, HAAA may request the modification of the current QoS profile present in the ASN. In such a case existing ISFs may require to be updated because of changed QoS parameters.

#### 4.6.4.3 Dynamic Service Flows

Dynamic service flows are defined as service flows which could be created, modified or deleted at any time during a session. Unlike Pre-Provisioned SFs, the creation of these service flows requires a specific authorization in addition

to admission and activation. When dynamic Service Flows are supported together with the PCC framework (see [3] for further details), policy / authorization check SHALL be performed by the PCRF.

#### **4.6.4.3.1 Create Service Flow**

In case of network initiated SF creation, the Anchor-SFA/A-PCEF may receive a request for service flow creation from the PCRF. The Anchor-SFA can assume that this request is authorized and SHALL try to create the service flow accordingly.

In case of MS initiated SF creation, the Anchor-SFA receives a request for a service flow creation from the SFM which might have been forwarded by a Serving-SFA. The Anchor-SFA has to verify the authorization which might be done with the help of the PCC framework. In this case, Anchor-SFA triggers the co-located A-PCEF to perform verification with the help of the PCRF. In case authorization check is done by the Anchor-SFA for non-PCC case, AAA has to provide a profile descriptor during the authentication procedure. The authorization check itself is implementation specific. Accounting of MS initiated SFs authorized by Anchor-SFA is similar to that of PPSFs. Accounting information need to be provided for each of the SF-profiles in the QoS profile.

#### **4.6.4.3.2 Delete Service Flow**

The Anchor-SFA/A-PCEF may receive a request for service flow deletion from the PCRF or the SFM (in case of graceful termination such as error conditions) or the MS. In such a case the Anchor-SFA SHALL trigger the service flow deletion accordingly. The Anchor-SFA SHALL forward the request to the co-located A-PCEF when PCC framework is used.

#### **4.6.4.3.3 Modify Service Flow**

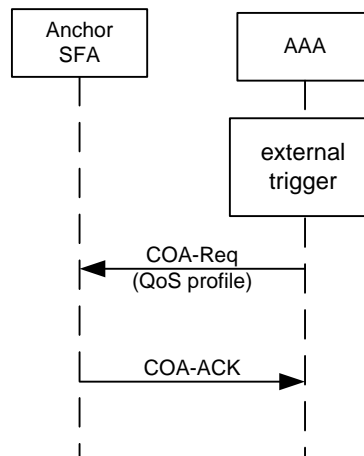
The Anchor-SFA/A-PCEF may receive a request for service flow modification from the PCRF or the SFM (which might be forwarded by a Serving-SFA). The Anchor-SFA can assume that this request is authorized and SHALL try to modify the service flow accordingly when the request was network initiated. In case of an MS or the SFM (which might be forwarded by a Serving-SFA) initiated request and an activated PCC framework, the Anchor-SFA SHALL forward the request to the co-located A-PCEF (when PCC framework is used) to inform the PCRF and obtain authorization. If the PCC framework was not activated, the Anchor-SFA SHALL perform the authorization check in an implementation specific manner.

#### **4.6.4.4 Data Path Handling**

The serving SFA SHALL trigger the establishment of the Data Path. The creation per SF SHALL be mandatorily supported.

#### 4.6.4.5 Message Flows and Flow Description

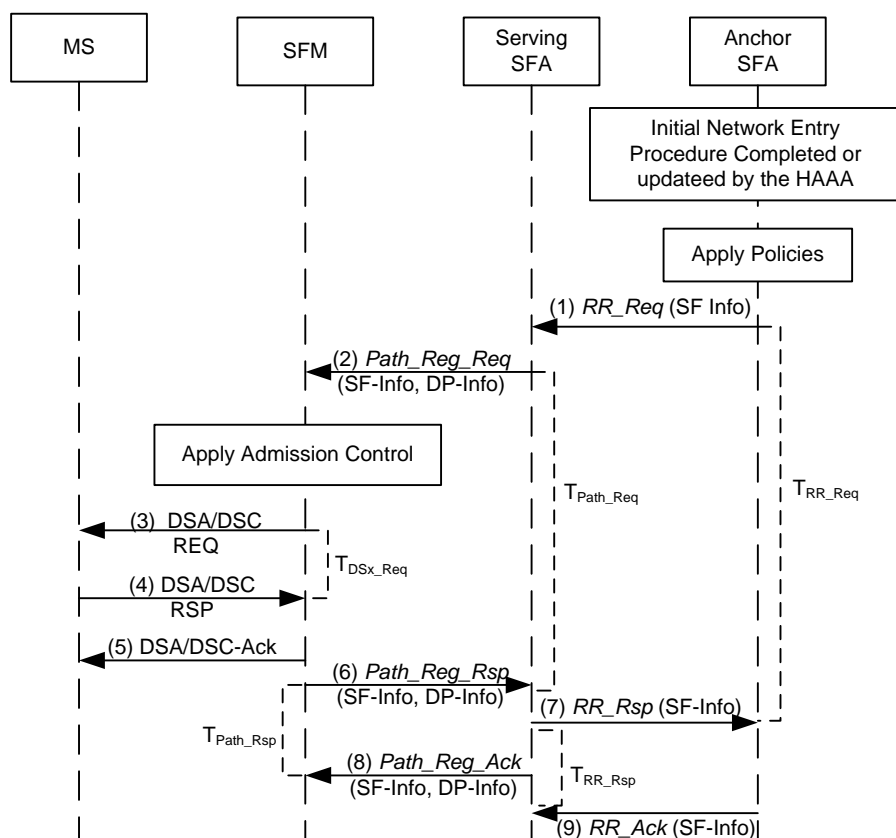
##### 4.6.4.5.1 Update of Pre-Provisioned QoS triggered by AAA



**Figure 4-71 – AAA-Triggered QoS Profile update**

Corresponding COA messages are defined in Table 5-6.

#### 4.6.4.5.2 Network Initiated Service Flow Creation/Modification



**Figure 4-72 – SFA-Triggered Service Flow Creation (Profile Downloaded in SFA)**

##### STEP 1

The initial QoS profile or a modification for it was received at the Anchor-SFA. *RR\_Req* according to Table 4-59 is sent to the Serving-SFA where the QoS-parameters are set according to the received QoS-profile.

##### STEP 2

Serving-SFA checks if a Data Path needs to be created. Depending on the result a *Path\_Reg\_Req* according to Table 4-67 (if a new DP is required) or a *Path\_Modification\_Req* according to (if an existing DP is used) is sent to the SFM. The *Path\_Reg\_Req* and *Path\_Modification\_Req* include the received QoS Parameters TLV received from the Anchor-SFA.

##### STEP 3

The SFM verifies whether there are sufficient radio resources and it decides (based on the QoS Parameters TLV and the available resources) whether the request should be accepted or not. In case of acceptance, a DSA-REQ according to IEEE802.16e [11] is sent to the MS.

##### STEP 4

MS accepts or rejects the DSA/DSC-REQ with a DSA/DSC-RSP according to IEEE802.16e [11].

##### STEP 5

SFM sends a DSA-ACK to the MS to complete the QoS transaction.

**STEP 6**

Assuming acceptance by SFM in step 3 and acceptance by MS in step 4 (i.e., confirmation code of DSA-RSP is OK/success) the SFM sends *Path\_Reg\_Rsp* or *Path\_Modification\_Rsp* messages according to Table 4-69 / Table 4-72 to the Serving SFA to confirm the reservation. In the case that reduced resources was granted by the SFM, the QoS parameter set of the granted resources SHALL be returned by the SFM in the response back to the Serving SFA.

**STEP 7**

In case of successful response from the SFM, the Serving SFA sends a *RR\_Rsp* message according to Table 4-64 with the QoS Parameters TLV containing granted QoS values to the Anchor SFA to confirm the reservation. A response message not matching to a sent request (e.g., if SFID of a *Path\_Reg\_Req* do not match to a received *Path\_Reg\_Rsp*) should be silently discarded.

**STEP 8**

A *Path\_Reg\_Ack* or *Path\_Modification\_Ack* is sent to the SFM.

**STEP 9**

In case of successful response from the Serving-SFA, the Anchor SFA sends back an *RR\_Ack*, as shown in section 5.2.1.3, to the Serving-SFA. No further action is necessary by the Anchor-SFA except to keep the context until the MS performs network exit.

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*) should be silently discarded.

#### 4.6.4.5.3 MS Initiated Service Flow Creation

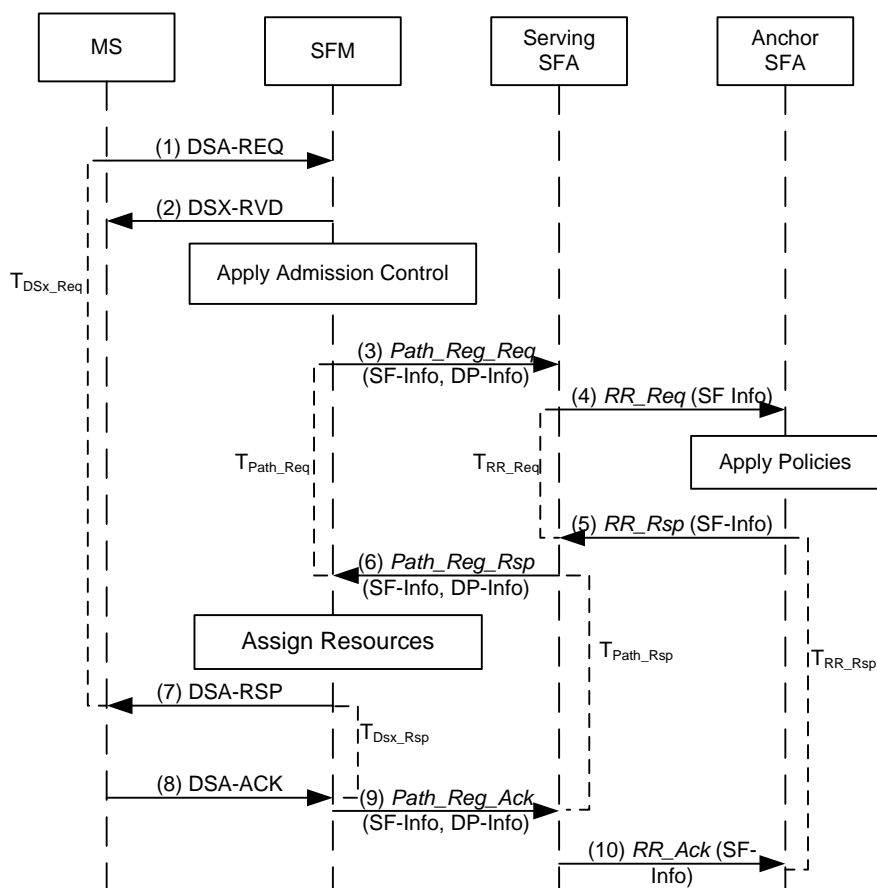


Figure 4-73 – MS Initiated Service Flow Creation

##### STEP 1

A DSA-REQ was received by the SFM from the MS.

##### STEP 2

According to IEEE802.16e [11] a DSX-RVD is sent to the MS.

##### STEP 3

The SFM verifies whether there are sufficient radio resources and it decides (based on the QoS-Info parameters and the available resources) whether the request should be accepted or not. In case of acceptance, SFM sends a *Path\_Registratoion\_Req* according to Table 4-68 to the Serving-SFA to trigger DP and SF reservation. The *Path\_Registratoion\_Req* include the QoS-Info TLV received from the MS.

##### STEP 4

*RR\_Req* according to Table 4-60 is sent to the Anchor-SFA where the QoS-parameters are set according to the received QoS-profile. The request will be forwarded to the co-located A-PCEF for the policy check when PCC framework is used.



**STEP 5**

In case of acceptance, the Anchor-SFA sends a *RR\_Rsp* message according to Table 4-64 with the QoS-Info parameters containing granted QoS values to the Serving-SFA to confirm the reservation. In the case that reduced resources was granted, the QoS parameter set of the granted resources SHALL be returned in the response back to the Serving SFA.

**STEP 6**

The Serving-SFA sends a *Path\_Registraton\_Rsp* messages according to Table 4-70 to the SFM to confirm the reservation.

**STEP 7**

The SFM confirms the request of the MS by DSA-RSP message.

**STEP 8**

MS sends a DSA-ACK to complete the QoS-request.

**STEP 9**

SFM sends a *Path\_Registration\_Ack* according to section Table 4-71 to the Serving-SFA to inform about the successful completion of the request.

**STEP 10**

The Anchor SFA receives an *RR\_Ack* as shown in section Table 4-66 to complete the QoS-request.

#### 4.6.4.5.4 MS Initiated Service Flow Modification

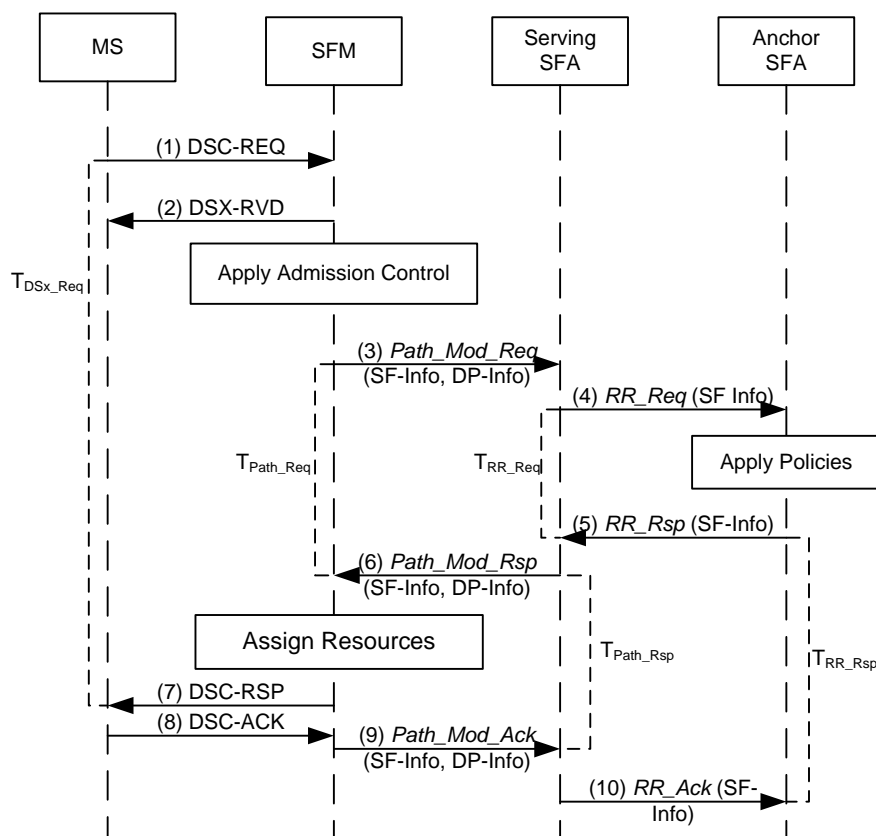


Figure 4-74 – MS initiated Service Flow Modification

##### STEP 1

A DSC-REQ was received by the SFM from the MS.

##### STEP 2

According to IEEE802.16e [11] a *DSX-RVD* is sent to the MS.

##### STEP 3

The SFM verifies whether there are sufficient radio resources and it decides (based on the QoS-Info parameters and the available resources) whether the request should be accepted or not. In case of acceptance, SFM sends a *Path\_Modification\_Req* (if an existing DP is used) according to Table 4-72 to the Serving-SFA. The *Path\_Modification\_Req* include the QoS-Info TLV received from the MS.

##### STEP 4

*RR\_Req* according to Table 4-59 is sent to the Anchor-SFA where the QoS-parameters are set according to what was received in the *Path\_Modification\_Req* message. The request will be forwarded to the co-located A-PCEF for the policy check and IP-CAN session modification when PCC framework is used.

##### STEP 5

In case that PCC is not activated Anchor-SFA verifies the QoS-request according to the subscriber profile received from AAA. In case of acceptance, the Anchor-SFA sends a *RR\_Rsp* message according to Table 4-64 with the QoS-Info parameters containing granted QoS values to the Serving-SFA to confirm the reservation. In the case that

reduced resources was granted, the QoS parameter set of the reduced resources SHALL be returned in the response back to the Serving SFA.

**STEP 6**

The Serving-SFA sends a *Path\_Modification\_Rsp* messages according to Table 4-72 to the SFM to confirm the reservation.

**STEP 7**

The SFM confirms the request of the MS by DSC-RSP message.

**STEP 8**

MS sends a DSC-ACK to complete the QoS-request.

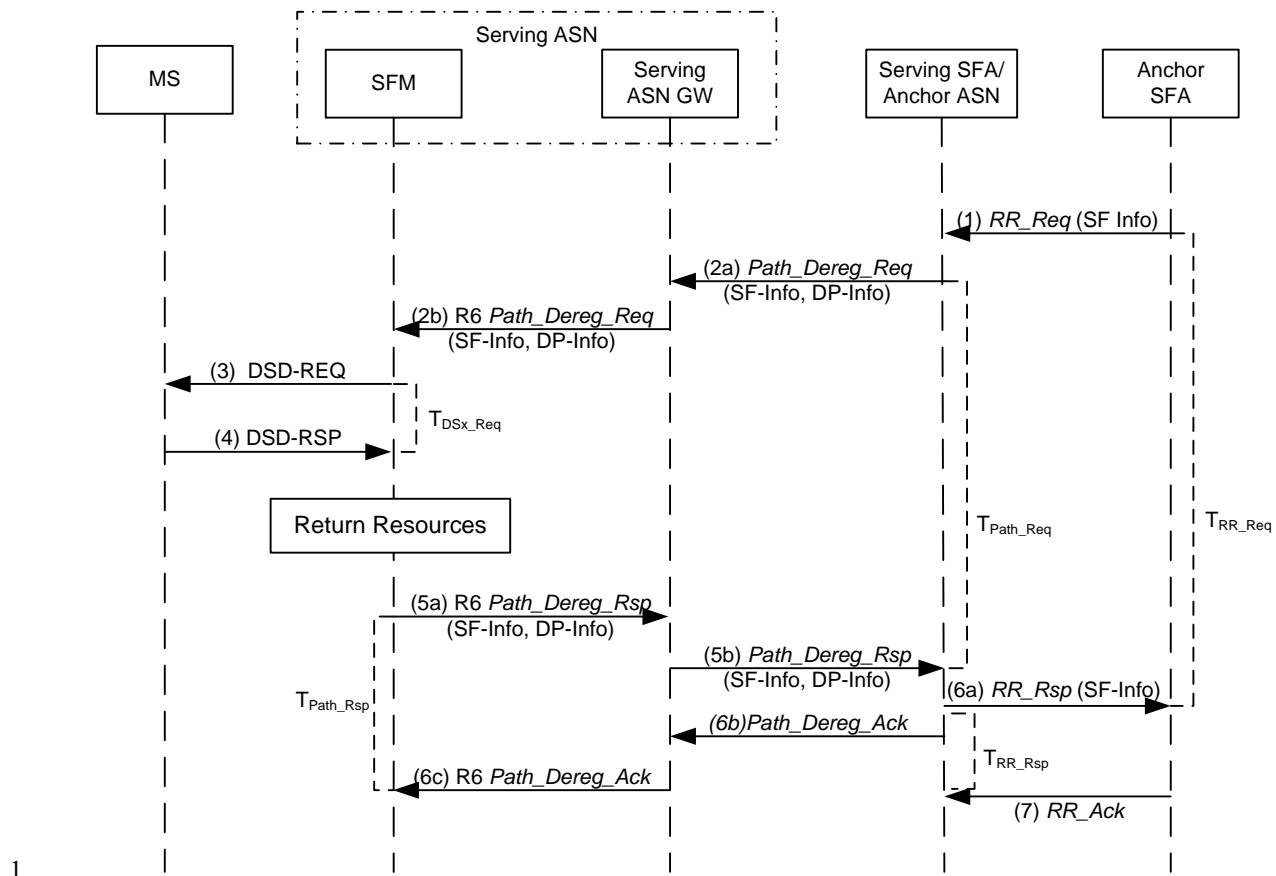
**STEP 9**

SFM sends a *Path\_Modification\_Ack* according to section Table 4-74 to the Serving-SFA to inform about the successful completion of the request.

**STEP 10**

The Anchor SFA receives an *RR\_Ack* as shown in section Table 4-66 to complete the QoS-request.

**4.6.4.5.5 Network Initiated Service Flow Deletion**



**Figure 4-75 – SFA-Triggered Service Flow Deletion**

### STEP 1

When a trigger for deletion of SF(s) received at the Anchor-SFA, the Anchor SFA sends an *RR\_Req* message according to Table 4-63 to the Serving-SFA where the SF(s) is (are) to be deleted.

### STEP 2

The Serving-SFA checks if a Data Path needs to be released. Depending on the result the Serving SFA sends a *Path\_Dereg\_Req* according to 4.6.5.4.4 to the SFM. The message includes the QoS Parameters TLV received from the Anchor-SFA. This message is relayed via Serving ASN GW to the SFM(BS).

### STEP 3

The SFM send a DSD-REQ according to IEEE802.16e [11] to the MS.

### STEP 4

The MS sends a DSD-RSP according to IEEE802.16e [11] back to the SFM.

### STEP 5

Upon receiving the response from the MS, the SFM sends *Path\_Dereg\_Rsp* message according to Table 4-76 to the Serving SFA to confirm the deletion. The message is relayed from the Serving ASN-GW to the SFA.

## STEP 6

Upon receiving a response from the SFM, the Serving SFA sends a *RR\_Rsp* message according to Table 4-65 to the Anchor SFA to confirm the service flow deletion. In addition, a *Path\_Dereg\_Ack* is sent to the SFM.

## STEP 7

Upon receipt of the *RR\_Rsp* with Reservation Result set to 0x0005, the Anchor-SFA SHALL release the context for the deleted SFs; a *RR\_Ack* according to Table 4-66 SHALL be sent to the Serving-SFA as acknowledgement.

### 4.6.4.5.6 MS Initiated Service Flow Deletion

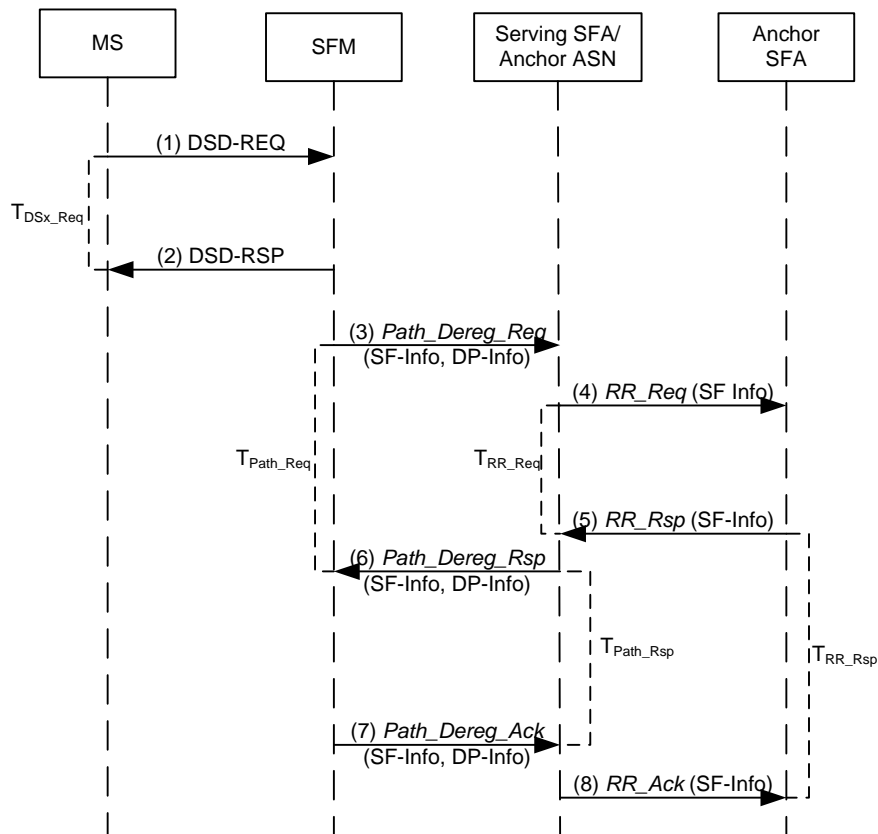


Figure 4-76 – MS-Triggered Service Flow Deletion

## STEP 1

The SFM receives DSD-REQ from MS.

## STEP 2

The SFM acknowledges the request for SF deletion if the corresponding resource was found by the SFM.

## STEP 3

The SFM send a *R6 Path\_Dereg\_Request* to the Serving-SFA.

#### STEP 4

The Serving-SFA sends an RR-Request to the Anchor-SFA indicating the deletion of an SF. The request will be forwarded to the co-located A-PCEF for IP-CAN session modification or termination when PCC framework is used.

#### STEP 5

The Anchor-SFA acknowledges the request with an RR-Response in case the referred resource was successfully removed.

#### STEP 6

The Serving-SFA sends an *R6 Path\_Dereg\_Response* to the SFM in case that the referred resource was successfully removed.

#### STEP 7

The SFM SHALL release the context for the deleted SFs and sends an *R6 Path\_Dereg\_Ack* to the Serving SFA to close the request.

#### STEP 8

The Serving-SFA SHALL release the context for the deleted SFs and SHALL send a *RR\_Ack* message according to Table 4-66 to the Anchor-SFA as an acknowledgement. The Anchor-SFA SHALL then also release the context.

#### 4.6.4.5.7 SF Management Timers and Timing Considerations

This section identifies the timer entities participating in the SF management procedure. The SF management procedure employs five timers (see Table 4-56):

- $T_{RR\_Req}$ : is started by an Anchor-SFA / a Serving-SFA upon sending a *RR\_Req* message. It is stopped upon receiving a corresponding *RR\_Rsp*.
- $T_{Path\_Req}$ : is started when the Serving-SFA / SFM sends a *Path\_Reg\_Req* and *Path\_Modification\_Req* and is stopped upon receiving a corresponding *Path\_Reg\_Rsp* and *Path\_Modification\_Rsp*.
- $T_{DSx\_Req}$ : is started by the SFM when DSA-REQ is sent on R1. It is stopped upon receiving a corresponding R1 DSA-RSP. It should be implemented according to  $T_7$  specified in IEEE802.16e.
- $T_{Path\_Rsp}$ : is started by the SFM / Serving-SFA when it sends a *Path\_Reg\_Rsp* and *Path\_Modification\_Rsp* message and is stopped upon receiving a corresponding *Path\_Reg\_Ack* and *Path\_Modification\_Ack* message.
- $T_{RR\_Rsp}$ : is started by the Serving SFA / Anchor-SFA when it sends a *RR\_Rsp* message and is stopped upon receiving a corresponding *RR\_Ack* message.

Table 4-56 shows the maximum value of timers and also indicates the range of the recommended duration of these timers. Note that these values are provisioned in the current Release.

**Table 4-56 – Timer Values for SF Management Procedure**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
$T_{RR\_Req}$			TBD
$T_{Path\_Req}$			TBD
$T_{DSx\_Req}$			1 sec <sup>1)</sup>

Timer	Default Values (msecs)	Criteria	Maximum Timer Value
T <sub>Path_Rsp</sub>			TBD
T <sub>RR_Rsp</sub>			TBD
T <sub>Dsx_Rsp</sub>			300msec <sup>2)</sup>

1) According to T<sub>7</sub> of IEEE802.16e.

2) According to T<sub>8</sub> of IEEE802.16e.

#### 4.6.4.5.8 SF Management Error Conditions

This section describes error conditions associated with the SF management procedure.

##### 4.6.4.5.8.1 Timer Expiry

The following table shows details on 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 4-57.

**Table 4-57 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T <sub>RR_Req</sub>	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 <sub>RR_Req</sub>	Serving SFA	The Serving SFA SHALL initiate network exit procedure.
T <sub>Path_Req</sub>	Serving SFA	Sends <i>RR_Rsp</i> message with Failure Indication TLV set to “Timer expired without response”.
T <sub>Path_Req</sub>	SFM	In the case of service flow addition or modification, the SFM SHALL send DSA/DSC-RSP with appropriate failure indication to the MS.
T <sub>DSx_Req</sub>	SFM	Sends <i>Path_Dereg_Rsp</i> and <i>Path_Modification_Rsp</i> with Failure Indication TLV set to “Timer expired without response”. In the case of SF deletion the SFM SHALL release the associated resources.
T <sub>Path_Rsp</sub>	SFM	The requested or deleted resources should be released. The deletion of the SFs on the MS should be triggered as described in [Figure 4-75] step 3 and 4.
T <sub>Path_Rsp</sub>	Serving SFA	The Serving SFA SHALL continue to assign the requested resources and release the resources that are deleted.
T <sub>RR_Rsp</sub>	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 4-75] step 2 to 5.
T <sub>Dsx_Rsp</sub>	SFM	Sends <i>Path_Reg_Ack</i> and <i>Path_Modification_Ack</i> with Failure Indication TLV set to “Timer expired without response”.

##### 4.6.4.5.8.2 Path\_Reg\_Rsp / Path\_Modification\_Rsp Error

Upon receipt of the *Path\_Reg\_Req* and *Path\_Modification\_Req* if the SFM determines that resources are unavailable or in case of non successful response of MS (confirmation code of DSA-RSP is different from OK/success), it SHALL send a *Path\_Reg\_Rsp* and *Path\_Modification\_Rsp* with the Failure Indication TLV with appropriate error code to the Serving-SFA. Upon receipt of the *Path\_Modification\_Req* if the SFM determines that

the modify request does not match an existing SF (e.g., the parameters of the *Path\_Modification\_Req* do not match any existing context), it SHALL send the *Path\_Modification\_Rsp* with the Failure Indication TLV set to “Requested Context Unavailable” to the serving-SFA. Note, when multiple Service flows are included in a single *Path\_Reg\_Req* or *Path\_Modification\_Req* message, the individual service flow failure may be indicated in the Reservation Result TLV.

Upon receipt of the *Path\_Reg\_Req* and *Path\_Modification\_Req* the Serving-SFA sends a *RR\_REQ* to the Anchor-SFA, and if the Serving-SFA receives an error *RR\_RSP* back from the Anchor-SFA, it SHALL send a *Path\_Reg\_Rsp* and *Path\_Modification\_Rsp* with the Failure Indication TLV with appropriate error code to the SFM. Upon receipt of the *Path\_Modification\_Req* if the Serving-SFA or the Anchor-SFA determine that the modify request does not match an existing SF (e.g., the parameters of the *Path\_Modification\_Req* do not match any existing context), the Serving-SFA (on its own or on response from the Anchor-SFA) SHALL send the *Path\_Modification\_Rsp* with the Failure Indication TLV set to “Requested Context Unavailable” to the SFM.

#### 4.6.4.5.8.3 RR\_Rsp Error

Upon receipt of the *RR\_Req* message to modify an existing context if the Serving-SFA determines that the modify request does not match an existing SF (e.g., the parameters of the *RR\_Req* do not match any existing context), it SHALL send the *RR\_Rsp* with the Failure Indication TLV set to “Requested Context Unavailable” to the Anchor-SFA.

Upon receipt of the *RR\_Req* message to modify an existing context if the Anchor-SFA determines that the modify request does not match an existing SF (e.g., the parameters of the *RR\_Req* do not match any existing context), it SHALL send the *RR\_Rsp* with the Failure Indication TLV set to “Requested Context Unavailable” to the Serving-SFA.

Upon receipt of the *Path\_Reg\_Rsp* and *Path\_Modification\_Rsp* with the Failure Indication TLV, the serving-SFA will stop timer  $T_{Path\_Req}$ . The serving-SFA may re-send the *Path\_Reg\_Req* and *Path\_Modification\_Req*. If the serving-SFA does not re-send the *Path\_Reg\_Req* and *Path\_Modification\_Req* message or if subsequent attempts are also unsuccessful, the serving-SFA SHALL send the *RR\_Rsp* message with Reservation Result TLV set to the appropriate error code value.

Upon receipt of the *Path\_Reg\_Rsp* and *Path\_Modification\_Rsp* with the Failure Indication TLV, the SFM will stop timer  $T_{Path\_Req}$ . The SFM may re-send the *Path\_Reg\_Req* and *Path\_Modification\_Req*. If the SFM does not re-send the *Path\_Reg\_Req* and *Path\_Modification\_Req* message or if subsequent attempts are also unsuccessful, the SFM SHALL send a *DSA-RSP* / *DSC-RSP* with an appropriate error response back to the MS.

Upon receipt of the *RR\_Rsp* message with Reservation Result TLV indicating non-successful response, the Anchor-SFA has to reject the network entry of the MS and SHALL trigger the Authenticator ASN to initiate network exit procedure and to send an Accounting Stop message including an error cause. The Anchor SFA will stop timer  $T_{RR\_Req}$ .

Upon receipt of the *RR\_Rsp* message with Reservation Result TLV indicating non-successful response, the Serving-SFA SHALL reject the request received from the SFM and send a *Path\_Reg\_Rsp* or *Path\_Modification\_Rsp* with Reservation Result TLV set to the appropriate error code value.

#### 4.6.5 QoS Messages

For QoS specific support, the ASN control plane function type header “0x01” as defined in section 5.2 SHALL be used. This section describes each QoS messages and their associated information elements (IE) in detail.

The following IEs are contained in this message, encoded in the TLV format. The notations (M) and (O) are used to indicate Mandatory and Optional, respectively.

##### 4.6.5.1 Messages and Information Elements (IEs) for QoS control in the ASN

QoS-related messages have been described in IEEE 802.16-2004 [10]. The general format of each such message is described in WiMAX End-to-End Network Systems Architecture Stage 2 [1].

QoS Control message IEs are combined with Data Path Control messages, when the QoS Control messages are sent along with the data path control messages over R4 and R6 reference points. Separate QoS resource reservation



messages may be sent for each group of service flows indicated by the combined resource indicator. The service flow creation, modification, and deletion QoS Control messages IEs SHOULD map to the following Data Path Control messages:

**Table 4-58 – Data Path Control Messages**

QoS Control Message	Data Path Control Message
<i>RR_Req</i> / <i>RR_Rsp</i> / <i>RR_Ack</i> (Create)	<i>Path_Reg_Req</i> , <i>Path_Reg_Rsp</i> and <i>Path_Reg_Ack</i> , or <i>Path_Modification_Req</i> , <i>Path_Modification_Rsp</i> , and <i>Path_Modification_Ack</i> if new SF uses existing DP.
<i>RR_Req</i> / <i>RR_Rsp</i> / <i>RR_Ack</i> (Modification)	<i>Path_Modification_Req</i> , <i>Path_Modification_Rsp</i> , and <i>Path_Modification_Ack</i> .
<i>RR_Req</i> / <i>RR_Rsp</i> / <i>RR_Ack</i> (Delete)	<i>Path_Dereg_Req</i> , <i>Path_Dereg_Rsp</i> and <i>Path_Dereg_Ack</i> , or <i>Path_Modification_Req</i> , <i>Path_Modification_Rsp</i> , and <i>Path_Modification_Ack</i> if DP is shared by another SF.

#### 4.6.5.2 RR\_Req

This message is sent from the Anchor-SFA to the Serving-SFA and in the opposite direction. A single *RR\_Req* message may include more than one SF-Info IE to allow the creation of more than one QoS service flow with a single request. *RR\_Req* message SHALL not be sent from Serving-SFA to SFM.

##### 4.6.5.2.1 Service Flow Creation or Modification (Anchor-SFA to Serving-SFA)

**Table 4-59 – RR\_Req: SF Creation or Modification (Anchor-SFA to Serving-SFA)**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
> Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS. The flag can be applied on a per MS level or per CS level. This TLV could have one or more instances dependent on the number of CS Types that are allowed for the MS and the level of the indication (i.e., per MS level or per CS level) that the flag is applied to. The details of the use of this TLV will be explained in the TLV's definition.
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	SHALL be set to "Create, Admit, Activate or Modify".

IE	Reference	M/O	Notes
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Correlation ID	5.3.2.37	O	This TLV SHALL be included for packet data flow based accounting.
>>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.
>>Paging Preference	5.3.2.262	O	MS's paging preference.
>>Packet Classification Rule/ Media Flow Description	5.3.2.114	M	Packet classifier as defined on R1. This parameter is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated.
>>>Classification Rule Index	5.3.2.30	M	Index assigned to the Packet Classification Rule.
>>>Classification Rule Action	5.3.2.31	O	Applies if SF modification.
>>> Classification 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	O	Allowed, but not restricted to, protocols are: TCP, UDP, ...
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>>MAC Source Address and Mask	5.3.2.384	O	See IEEE802.16e for further details.
>>>MAC Destination Address and Mask	5.3.2.385	O	See IEEE802.16e for further details.
>>>ETYPE/SAP	5.3.2.386	O	See IEEE802.16e for further details.
>>>User Priority Range	5.3.2.387	O	See IEEE802.16e for further details.
>>>SVLAN ID	5.3.2.393	O	SVLAN ID is only applied for DL classification
>>>CVLAN ID	5.3.2.394	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>> DSCP	5.3.2.409	O	TC bit is set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.

IE	Reference	M/O	Notes
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>> Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).

IE	Reference	M/O	Notes
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>Media Flow Type	5.3.2.94	O	
>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>Reduced Resources Code	5.3.2.237	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHS Rule Action	5.3.2.128	CM	Mandatory if PHS-Rules are present.
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	This TLV SHALL be included if BS Info is included in the transmitted message.

1

#### 2 4.6.5.2.2 Service Flow Creation (Serving-SFA to Anchor-SFA)

3

**Table 4-60 – RR\_Req: SF Creation (Serving-SFA to Anchor-SFA)**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
> Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS. The flag can be applied on a per MS level or per CS level. This TLV could have one or more instances dependent on the number of CS Types that are allowed for the MS and the level of the indication (i.e. per MS level or per CS level) that the flag is applied to. The details of the use of this TLV will be explained in the TLV's definition.
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.

IE	Reference	M/O	Notes
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	
>>Reservation Action	5.3.2.151	M	SHALL be set to “Create, Admit, Activate or Modify”.
>>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/ Media Flow Description	5.3.2.114	M	Packet classifier as defined on R1. This parameter is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated.
>>> Classification Rule Index	5.3.2.30	M	
>>> Classification 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, ... OPTIONAL for wildcard classifiers
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>>MAC Source Address and Mask	5.3.2.384	O	See IEEE802.16e for further details.
>>>MAC Destination Address and Mask	5.3.2.385	O	See IEEE802.16e for further details.
>>>ETYPE/SAP	5.3.2.386	O	See IEEE802.16e for further details.
>>>User Priority Range	5.3.2.387	O	See IEEE802.16e for further details.
>>>SVLAN ID	5.3.2.393	O	SVLAN ID is only applied for DL classification
>>>CVLAN ID	5.3.2.394	O	See IEEE802.16e for further details.

IE	Reference	M/O	Notes
>>QoS Parameters	5.3.2.141	M	
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	
>>>>Maximum Latency	5.3.2.91	CM	
>>>>Unsolicited Grant Interval	5.3.2.199	CM	
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	
>>>>Maximum Latency	5.3.2.91	CM	
>>>>Unsolicited Polling Interval	5.3.2.200	CM	
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>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 Code	5.3.2.237	O	
>>PHS Rule	5.3.2.127	M	
>>>PHSI	5.3.2.125	M	Mandatory if PHS-Rules are present.
>>>PHSS	5.3.2.129	M	Mandatory if PHS-Rules are present.

IE	Reference	M/O	Notes
>>>PHSF	5.3.2.124	M	Mandatory if PHS-Rules are present.
>>>PHSM	5.3.2.126	M	Mandatory if PHS-Rules are present.
>>>PHSV	5.3.2.130	M	Mandatory if PHS-Rules are present.
>>>PHS Rule Action	5.3.2.128	M	Mandatory if PHS-Rules are present.

#### 4.6.5.2.3 Service Flow Modification for state change (Serving-SFA to Anchor-SFA)

Service Flow Modification is separated into two cases.

Modification of the flow state (to change between Provisioned, Admitted and Active state)

Modification of any service flow parameter

Modification of flow state is a mandatory feature where the free modification of other parameters is an optional feature. Modification of parameters is limited according to IEEE802.16e [11].

**Table 4-61 – RR\_Req: SF Modification, state change only (Serving-SFA to Anchor-SFA)**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	SHALL be set to “Admit, Activate or Modify”.
>>SFID	5.3.2.184	M	SFID as defined on R1.

Following definition show the message where any parameter could be modified.

**Table 4-62 – RR\_Req: SF Modification (Serving-SFA to Anchor-SFA)**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
> Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS. The flag can be applied on a per MS level or per CS level. This TLV could have one or more instances dependent on the number of CS Types that are allowed for the MS and the level of the indication (i.e. per MS level or per CS level) that the flag is applied to. The details of the use of this TLV will be explained in the TLV’s definition.
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	SHALL be set to “Create, Admit, Activate or Modify”.

IE	Reference	M/O	Notes
>>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/ Media Flow Description	5.3.2.114	M	Packet classifier as defined on R1. This parameter is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated.
>>>Classification Rule Index	5.3.2.30	M	Index assigned to the Packet Classification Rule
>>>Classification Rule Action	5.3.2.31	O	Applies if SF modification
>>> Classification 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, ... OPTIONAL for wildcard classifiers
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>>MAC Source Address and Mask	5.3.2.384	O	See IEEE802.16e for further details.
>>>MAC Destination Address and Mask	5.3.2.385	O	See IEEE802.16e for further details.
>>>ETYPE/SAP	5.3.2.386	O	See IEEE802.16e for further details.
>>>User Priority Range	5.3.2.387	O	See IEEE802.16e for further details.
>>>SVLAN ID	5.3.2.393	O	SVLAN ID is only applied for DL classification
>>>CVLAN ID	5.3.2.394	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service



IE	Reference	M/O	Notes
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	
>>>>Maximum Latency	5.3.2.91	CM	
>>>>Unsolicited Grant Interval	5.3.2.199	CM	
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	
>>>>Maximum Latency	5.3.2.91	CM	
>>>>Unsolicited Polling Interval	5.3.2.200	CM	
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>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 Code	5.3.2.237	O	
>>PHS Rule	5.3.2.127	M	
>>>PHSI	5.3.2.125	M	Mandatory if PHS-Rules are present.
>>>PHSS	5.3.2.129	M	Mandatory if PHS-Rules are present.
>>>PHSF	5.3.2.124	M	Mandatory if PHS-Rules are present.
>>>PHSM	5.3.2.126	M	Mandatory if PHS-Rules are present.
>>>PHSV	5.3.2.130	M	Mandatory if PHS-Rules are present.
>>>PHS Rule Action	5.3.2.128	M	Mandatory if PHS-Rules are present.

#### 4.6.5.2.4 Service Flow Deletion

**Table 4-63 – 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	SHALL be set to “Delete”.
>>SFID	5.3.2.184	M	SFID as defined on R1.
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	This TLV SHALL be included if BS Info is included in the transmitted message.

#### 4.6.5.3 RR\_Rsp

This message is sent in response to an *RR\_Req*. Depending on the request it is sent by the serving SFA to the anchor SFA or in the opposite direction. *RR\_Rsp* SHOULD include the SF-Info and the result code of the reservation request. The *RR\_Rsp* message should not be sent from SFM to the serving SFA.

#### 4.6.5.3.1 Service Flow Creation

**Table 4-64 – RR\_Rsp: SF Creation**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
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	
>>Packet Classification Rule/ Media Flow Description	5.3.2.114	O	Packet classifier as defined on R1. This parameter is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated. It has to be present in response messages sent from Anchor-SFA to Serving-SFA as far as a classifier was present in the request.
>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule. It must be present for each classification rule which was present in the request as far as the response is sent from Anchor-SFA to Serving-SFA.
>>QoS Parameters	5.3.2.141	O	In case of network-initiated service flows, this is only allowed to be present if “Reduced Resources Code” was set at the corresponding <i>RR_Req</i>

IE	Reference	M/O	Notes
			message.
>>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery service.
>>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted

IE	Reference	M/O	Notes
			message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.

#### 4.6.5.3.2 Service Flow Deletion

Table 4-65 – RR\_Rsp: Deletion of a SF

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
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	

#### 4.6.5.3.3 RR\_Ack

Table 4-66 – RR\_Ack

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
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.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

#### 4.6.5.4 Combined Data Path and QoS Control Messages IEs

The parameters of *RR\_Req/RR\_Rsp* messages are exchanged by Data Path Control messages between SFM and Serving-SFA.

##### 4.6.5.4.1 Combined Service Flow Creation

*Path\_Reg\_Req*, *Path\_Reg\_Rsp* and *Path\_Reg\_Ack*, messages SHOULD be used to create service flow and data path. *Path\_Reg\_Req* message is sent from the AnchorDP/serving SFA to the Serving DP/SFM. A single *Path\_Reg\_Req* or *Path\_Prereg\_Req* message may include more than one SF-Info TLV to allow the creation of more than one QoS service flow with a single request. The formats of *Path\_Reg\_Req*, *Path\_Reg\_Rsp*, *Path\_Reg\_Ack* message and their message types are defined in the section 5.2.3.

1

**Table 4-67 – Path-Reg-Req: Creation of SF and DP (network initiated)**

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).
> Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS. The flag can be applied on a per MS level or per CS level. This TLV could have one or more instances dependent on the number of CS Types that are allowed for the MS and the level of the indication (i.e., per MS level or per CS level) that the flag is applied to. The details of the use of this TLV will be explained in the TLV's definition.
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	SHALL be set to “Create, Admit & Activate”.
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Direction	5.3.2.59	M	Specifies the direction of the reservation.
>>Correlation ID	5.3.2.37	O	This TLV SHALL be included for packet data flow based accounting.
>>CID	5.3.2.29	O	This identifier is only mandatory if a DataPath of Type 2 is used between SFA and SFM. Note: Type 2 DataPath is optional.
>>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	5.3.2.262	O	Indicates paging preference.
>>Packet Classification Rule/ Media Flow Description	5.3.2.114	O	Packet classifier as defined on R1. This parameter is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated.
>>>Classification Rule Index	5.3.2.30	CM	This TLV SHALL be included if Packet Classification Rule/ Media Flow Description is included in the transmitted message. Index assigned to the Packet Classification Rule.
>>>Classification Rule Priority	5.3.2.32	O	See IEEE802.16e for further details.

IE	Reference	M/O	Notes
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	O	Allowed, but not restricted to, protocols are: TCP, UDP, ...
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>>MAC Source Address and Mask	5.3.2.384	O	See IEEE802.16e for further details.
>>>MAC Destination Address and Mask	5.3.2.385	O	See IEEE802.16e for further details.
>>>ETYPE/SAP	5.3.2.386	O	See IEEE802.16e for further details.
>>>User Priority Range	5.3.2.387	O	See IEEE802.16e for further details.
>>>SVLAN ID	5.3.2.393	O	SVLAN ID is only applied for DL classification
>>>CVLAN ID	5.3.2.394	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>>DSCP	5.3.2.409	O	TC bit is set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery service.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if BE Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted

IE	Reference	M/O	Notes
			message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>> Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.

IE	Reference	M/O	Notes
>>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>>Media Flow Type	5.3.2.94	O	
>>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>>Reduced Resources Code	5.3.2.237	O	
>>>>Data Path Info	5.3.2.45	O	Data Path Info TLV SHALL be Present for the Service Flow which the Sender is responsible for creating.
>>>>Data Path ID	5.3.2.44	CM	
>>>>Tunnel Endpoint	5.3.2.194	O	
>>>>SDU Info	5.3.2.176	O	Only be present if SDU should be supported.
>>>>SDU SN	5.3.2.178	CM	This TLV SHALL be included if SDU Info is included in the transmitted message.
>>>>SDU BSN Map	5.3.2.175	O	
>>>>PHS Rule	5.3.2.127	O	
>>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.



IE	Reference	M/O	Notes
>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHS Rule Action	5.3.2.128	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

1

2

**Table 4-68 – Path-Reg-Req: Creation of SF and DP (MS initiated)**

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)
> Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS. The flag can be applied on a per MS level or per CS level. This TLV could have one or more instances dependent on the number of CS Types that are allowed for the MS and the level of the indication (i.e. per MS level or per CS level) that the flag is applied to. The details of the use of this TLV will be explained in the TLV's definition.
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	
>>Reservation Action	5.3.2.151	M	MUST be set to "Create"
>>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. Note: Type 2 DataPath is optional.
>>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	5.3.2.262	O	Indicates paging preference.

IE	Reference	M/O	Notes
>>Packet Classification Rule/ Media Flow Description	5.3.2.114	O	Packet classifier as defined on R1. This parameter is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated.
>>>Classification Rule Index	5.3.2.30	CM	
>>>Classification 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, ... OPTIONAL for wildcard classifiers
>>>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 Parameter	7.3.2.1 of [8]	O	See [8]for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>>MAC Source Address and Mask	5.3.2.384	O	See IEEE802.16e for further details.
>>>MAC Destination Address and Mask	5.3.2.385	O	See IEEE802.16e for further details.
>>>ETYPE/SAP	5.3.2.386	O	See IEEE802.16e for further details.
>>>User Priority Range	5.3.2.387	O	See IEEE802.16e for further details.
>>>SVLAN ID	5.3.2.393	O	SVLAN ID is only applied for DL classification
>>>CVLAN ID	5.3.2.394	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>> DSCP	5.3.2.409	O	TC bit is set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery service
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service

IE	Reference	M/O	Notes
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>> Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.

IE	Reference	M/O	Notes
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	See IEEE802.16e for further details.
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>Media Flow Type	5.3.2.94	O	
>>>Reduced Resources Code	5.3.2.237	O	
>>Data Path Info	5.3.2.45	M	Identifies the Data Path which SHALL be used for the service flow.
>>>Data Path ID	5.3.2.44	M	
>>>Tunnel Endpoint	5.3.2.194	O	
>>SDU Info	5.3.2.176	O	Only be present if SDU should be supported.
>>>SDU SN	5.3.2.178	CM	
>>>SDU BSN Map	5.3.2.175	O	
>>>PHS Rule	5.3.2.127	M	
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSS	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHS Rule Action	5.3.2.128	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>BS Info	5.3.2.26	O	
>>BS ID	5.3.2.25	CM	

1

2

**Table 4-69 – Path-Reg-Rsp: Creation of SF and DP (network initiated)**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Registration Type	5.3.2.145	M	

IE	Reference	M/O	Notes
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. Note: Type 2 DataPath is optional.
>>Reservation Result	5.3.2.152	M	
>>QoS Parameters	5.3.2.141	O	This is only allowed to be present if “Reduced Resources Code” was set at the corresponding <i>RR_Req</i> message.
>>>DSCP	5.3.2.409	O	TC bit is set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery service.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	See IEEE802.16e for further details.
>>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>> Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details..
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.

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

IE	Reference	M/O	Notes
>>Data Path Info	5.3.2.45	O	Compound TLV including information about Data Path. Data Path Info TLV SHALL be Present only for the Service Flow which the Sender is responsible for creating.
>>>Data Path ID	5.3.2.44	CM	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.
>>>Tunnel Endpoint	5.3.2.194	O	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

1

**Table 4-70 – Path-Reg-Rsp: Creation of SF and DP (MS initiated)**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
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. Note: Type 2 DataPath is optional.
>>Reservation Result	5.3.2.152	M	
>>Packet Classification Rule/ Media Flow Description	5.3.2.114	O	Packet classifier as defined on R1. This parameter is mandatory for n-1 SFs which are in Active state. This parameter is optionally if the SF will not already be activated. It has to be present in response messages sent from Serving-SFA to BS as far as a classifier was present in the request.
>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule. It must be present for each classification rule which was present in the request as far as the response is sent from Serving-SFA to BS.
>>QoS Parameters	5.3.2.141	O	In the case of network-initiated service flows, this is only allowed to be present if “Reduced Resources Code” was set at the corresponding <i>RR_Req</i> message.
>>> DSCP	5.3.2.409	O	TC bit is set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery service

IE	Reference	M/O	Notes
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if BE Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>> Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.



IE	Reference	M/O	Notes
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message for service flow establishment. See IEEE802.16e for further details.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>Data Path Info	5.3.2.45	M	Compound TLV including information about Data Path.
>>>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
>>>Tunnel Endpoint	5.3.2.194	O	
>>Tunnel Endpoint	5.3.2.194	O	
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	

1

2

**Table 4-71 – Path-Reg-Ack: Creation of SF and DP**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
BS Info	5.3.2.26	M	

IE	Reference	M/O	Notes
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation. Included during IM Mode Exit procedure.
> Serving/Target Indicator	5.3.2.182	M	Set to “Serving”.

#### 4.6.5.4.2 Combined Service Flow Modification

*Path\_Modification\_Req*, *Path\_Modification\_Rsp* and *Path\_Modification\_Ack* messages SHOULD be used to modify a service flow and its related data path. *Path\_Modification\_Req* message is sent from the AnchorDP/serving SFA to the ServingDP/SFM. A single *Path-Modification-Req* message may include more than one SF-Info TLV to allow the modification of more than one QoS service flow with a single request.

#### 4.6.5.4.3 In Case of Modification of a SF and the Related DP

**Table 4-72 – Path-Modification-Req: 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 ASN GW ID	5.3.2.10	M	Unique Identifier of the Anchor GW (Anchor DP entity).
> Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resources Required flag is enabled or not for this MS. The flag can be applied on a per MS level or per CS level. This TLV could have one or more instances dependent on the number of CS Types that are allowed for the MS and the level of the indication (i.e., per MS level or per CS level) that the flag is applied to. The details of the use of this TLV will be explained in the TLV’s definition.
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.
>SF Info	5.3.2.185	M	
>>Reservation Action	5.3.2.151	M	SHALL be set to “Modify”.
>>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.

IE	Reference	M/O	Notes
>>>Packet Classification Rule/ Media Flow Description	5.3.2.114	O	Packet classifier as defined on R1. This parameter is mandatory for n-1 SFs when set to Active state. This parameter is optionally if the SF will not already be activated.
>>>>Classification Rule Index	5.3.2.30	CM	This TLV SHALL be included if Packet Classification Rule/ Media Flow Description is included in the transmitted message. Index assigned to the Packet Classification Rule.
>>>>Classification Rule Action	5.3.2.31	O	Applies if SF modification.
>>>> Classification 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.
>>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>>>MAC Source Address and Mask	5.3.2.384	O	See IEEE802.16e for further details.
>>>>MAC Destination Address and Mask	5.3.2.385	O	See IEEE802.16e for further details.
>>>>ETYPE/SAP	5.3.2.386	O	See IEEE802.16e for further details.
>>>>User Priority Range	5.3.2.387	O	See IEEE802.16e for further details.
>>>>SVLAN ID	5.3.2.393	O	SVLAN ID is only applied for DL classification
>>>>CVLAN ID	5.3.2.394	O	See IEEE802.16e for further details.
>>>QoS Parameters	5.3.2.141	O	
>>>> DSCP	5.3.2.409	O	TC bit is set to 1
>>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery service.
>>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.

IE	Reference	M/O	Notes
>>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>> Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.

IE	Reference	M/O	Notes
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>Media Flow Type	5.3.2.94	O	
>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>Reduced Resources Code	5.3.2.237	O	
>>Data Path Info	5.3.2.45	O	Identifies the Data Path which should be used for the service flow. Data Path Info TLV SHALL be Present only for the Service Flow which the Sender is responsible for creating.
>>>Data Path ID	5.3.2.44	CM	
>>>Data Path Type	5.3.2.47	O	
>>>Tunnel Endpoint	5.3.2.194	O	
>>SDU Info	5.3.2.176	O	Only be present if SDU should be supported.

IE	Reference	M/O	Notes
>>>SDU SN	5.3.2.178	CM	This TLV SHALL be included if the SDU Info is included in the transmitted message.
>>>SDU BSN Map	5.3.2.175	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHS Rule Action	5.3.2.128	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

**Table 4-73 – Path-Modification-Rsp: Modification of SF and DP**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
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. Note: Type 2 DataPath is optional.
>>Reservation Result	5.3.2.152	M	

IE	Reference	M/O	Notes
>>QoS Parameters	5.3.2.141	O	In the case of network-initiated service flows, this is only allowed to be present if “Reduced Resources Code” was set at the corresponding <i>RR_Req</i> message.
>>>DSCP	5.3.2.409	O	TC bit is set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery service.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	CM	See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>> Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details..
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.

IE	Reference	M/O	Notes
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>Data Path Info	5.3.2.45	O	Compound TLV including information about Data Path. Data Path Info TLV SHALL be Present only for the Service Flow which the Sender is responsible for creating.
>>>Data Path ID	5.3.2.44	CM	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.
>>>Tunnel Endpoint	5.3.2.194	O	



IE	Reference	M/O	Notes
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	This TLV SHALL be included if BS Info is included in the transmitted message.

**Table 4-74 – Path-Modification-Ack: Modification of SF and DP**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation. Included during IM Mode Exit procedure.
> Serving/Target Indicator	5.3.2.182	M	Set to “Serving”.

#### 4.6.5.4.4 Combined Service Flow Deletion

*Path\_Dereg\_Req* message is sent from the AnchorDP/serving SFA to the ServingDP/SFM or from the ServingDP/SFM to the AnchorDP/serving SFA. A single *Path\_Dereg\_Req* message may include more than one SF-Info TLV to allow the deletion of more than one QoS service flow with a single request. The formats of *Path\_Dereg\_Req*, *Path\_Dereg\_Rsp*, and *Path\_Dereg\_Ack* message and their message types are defined in the section 5.2.3.

**Table 4-75 – Path\_Dereg\_Req: Deletion of SF and DP**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
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.
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	This TLV SHALL be included if BS Info is included in the transmitted message.

**Table 4-76 – Path\_Dereg\_Rsp: Deletion of Service Flow and DP**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Registration Type	5.3.2.145	M	Describes type of the Registration.
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.
>>>Reservation Result	5.3.2.152	M	
>>>>Tunnel Endpoint	5.3.2.194	O	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

**Table 4-77 – Path\_Dereg\_Ack: Deletion of Service Flow and DP**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

#### 4.6.6 SFID Management

The Anchor/Serving SFA takes care of SFID assignment on the Service Flows. An SFID SHALL uniquely represent a Service Flow within the MS.

Thus the Anchor/Serving SFA SHALL keep track of the SFIDs that have been already assigned to the MS. This is possible because the SFA is by definition the entity that takes care of service authorization for each particular MS. Thus the Anchor/Serving SFA simply assigns a new SFID by selecting a value, which is not yet in use in the MS with which the Service Flow is associated. This discipline guarantees that {MSID, SFID} pair is unique network wide.

If the Anchor/Serving SFA initiates Service Flow creation, then the SFIDs are delivered to the SFM with DP-Registration Request sent from the Anchor/Serving SFA to the SFM. The SFM (in the Base Station) then uses the assigned SFIDs in the IEEE 802.16e DSx message exchange with the MS.

Upon a Service Flow release the Anchor/Serving SFA releases the associated SFID, which might be reused later for another, newly created, Service Flow.

The SFID assignment for MBS services is defined by the specification for MCBCS support in Mobile WiMAX.

#### 4.6.7 QoS Profile in the MS

MS MAY be configured with QoS profile. This configuration MAY happen via Over-the-Air Provisioning procedures, preconfiguration, or via other configuration means. Support for this configuration is optional in the MS as well as in the network side.

Per operator policy, QoS profile MAY be configured in the MS whenever QoS Profile of the subscriber is created or changes. It is implementation specific how the MS uses QoS profile in determining QoS attributes for formulating SF creation or modification requests.

The following parameters MAY be included in the QoS profile in the MS:

- TotalTrafficRate: Maximum value of sum of Maximum Sustained Traffic Rate parameters of existing SFs created by MS. This parameter is optional.
- Service Flow (zero or more)
  - Number of SFs: Number of this kind of SFs that the MS is allowed to create. This parameter is optional.
  - List of Service Types (zero or more)
    - Service Type: Intended to be carried over this kind of SF. This is provided as specified in RFC4288. The format is derived from the Content-Type of RFC2045 where only the “type” and “subtype” will be provided. In the Augmented BNF notation of RFC 822, the content-type value is defined as follows:  

ServiceType := type “/” subtype

The notation for “type” and “subtype” is specified in RFC4288.

This parameter is optional.
  - Direction (UL/DL): Direction of the SF. This parameter is mandatory.
  - Scheduling Type: Scheduling type of the SF. This parameter is mandatory.
  - Maximum Sustained Traffic Rate: Maximum value of maximum sustained traffic rate that the MS is allowed to use per this SF profile. This parameter is optional.
  - Minimum Reserved Traffic Rate: Maximum value of minimum reserved traffic rate that the MS is allowed to use per this SF profile. This parameter is optional.
  - Maximum Latency: Minimum value of maximum latency that the MS is allowed to use per this SF profile. This parameter is optional.

## 4.7 ASN Anchored Mobility

### 4.7.1 Introduction

The ASN consists of one or more BSs and one or more ASN GWs. The BSs SHALL be connected to the ASN GWs with R6 interfaces. The ASN GWs are interconnected with R4 interfaces. The ASN entities involved in a handover include the following:

- a. Serving BS that hosts Serving HO Function and serves the MS prior to HO.
- b. Target BS that hosts Target HO Function. There might be one or more Target BSs. One of them is selected as the final HO Target and becomes Serving BS after HO completion.
- c. Relay ASN GW that relays the HO Control messages between the Serving and Target BSs over R6. The Relay ASN-GW is an abstract functionality and in implementation can also take the role of any ASN GW that has an R6 interface with the Serving or Target BSs (e.g., Serving or Target ASN GWs). There could be multiple Relay ASN GWs involved in relaying HO Control Messages for a certain MS. The Relay ASN-GW can also be a stateless or stateful relay. These are left as implementation options.
- d. Anchor ASN-GW that hosts the Anchor DP Function for the MS. Serving ASN GW MAY be located on the path between Anchor ASN GW and Serving BS. The Target ASN GW MAY be located on the path between the Anchor ASN GW and the Target BS. In this case each such Data Path has R6 segment and R4 segment.
- e. Authenticator ASN-GW that hosts Authenticator/Key Distributor Function for the MS.

All ASN-GWs involved in HO SHALL be interconnected with R4 interfaces.

Data integrity may be optionally applied during the HO procedure to minimize or prevent data loss as a result of the HO.

## 4.7.2 Fully Controlled HO

### 4.7.2.1 HO Preparation Phase

Upon reception of a MOB-MSHO\_REQ message from a mobile station (MS), the Serving BS SHALL initiate a handover to one or more candidate Target BSs by sending an *HO\_Req* message to each Target BS over the R6 interface. If a target BS is connected to another ASN-GW, the *HO\_Req* message is relayed over R4 to the target BS. The Relay ASN-GW SHALL relay the message(s) to the Target BS(s) over the R6/R4 interface(s). If no acceptable target BS is available, the Serving BS sends a *MOB\_BSHO-RSP* message to the MS containing no potential target BS to reject the handover. If the MS mobility access classifier is fixed or nomadic and the BS supports mobility restriction for stationary access, only Target BSs that belong to the MS Reattachment zone may be selected for a handover.

If the MS sends a MOB\_MSHO-REQ to the serving BS without including any preferred target BSs, the serving BS MAY respond with a MOB\_BSHO-RSP message with the Mode field set to '0b111' (MS handover request not recommended [BS in list unavailable]), or the serving BS MAY select and recommend a target BS(s) to the MS in the MOB\_BSHO-RSP message.

The Serving BS SHALL silently discard duplicate *MOB\_MSHO-REQ* message from an MS if it has already initiated the HO preparation phase for the MS. If a Serving BS receives a duplicate *MOB\_MSHO-REQ* from an MS, it SHALL not propagate the request further in to the network.

A Relay ASN-GW involved in the handover has no handover related intelligence, therefore the Serving BS SHALL be required to send a separate R6 *HO\_Req* message for each potential Target BS.

The *HO\_Req* message SHALL contain an Authenticator ID TLV that points to the Authenticator/Key Distributor Function hosted in the Authenticator ASN-GW. Thus upon receiving a *HO\_Req* message, the Target BS(s) MAY retrieve AK context from the Authenticator ASN-GW. The Target BS(s) is/are not required to retrieve this information immediately upon receipt of the *HO\_Req* message and MAY postpone the retrieval until the Handover Action Phase. This call flow scenario (subsequently referred to as Scenario 1) is shown in Figure 4-77.

If the Authenticator is co-located at the Serving ASN-GW, the Serving ASN-GW MAY piggyback the AK Context on to the *HO\_Req* message.

If the MS mobility access classifier is fixed or nomadic, the MS' Authenticator SHALL reject AK context requests for/from the unauthorized Target BSs based on Authenticator's knowledge of MS Reattachment Zone list. To reject the AK context request for/from the Target BS, the MS' Authenticator responds with Context-Rpt message that includes appropriate Failure Indication value and excludes MS' AK context.

The Serving BS may have no knowledge with respect to whether authenticator or data path functions are co-located at the Serving ASN-GW. The Serving BS has no knowledge with respect to whether the Serving ASN-GW is using a stateless relay mode or a stateful relay mode.

The TEK context information may be transferred from Serving BS to Target BS if they are in the same mobility domain.

The *HO\_Req* message shall include the Anchor ASN GW ID hosting the data path function. The Target BS(s) MAY pre-establish the data path for the MS with the Anchor ASN-GW. If the Target BS(s) decides to pre-establish the data path, the Target BS SHALL initiate Data Path Pre-Registration procedure with the Anchor ASN-GW by sending a *Path\_Prereg\_Req* message to the Anchor ASN-GW. This call flow scenario is shown in Figure 4-77.

Data Path Pre-Registration at the Handover Preparation Phase is optional and may be executed only when both Target and Anchor ASN-GW support this functionality. If the Anchor ASN-GW does not support Data Path Pre-Registration and the Target BS attempts to initiate Data Path Pre-Registration procedure, the transaction should be rejected (i.e., *Path\_Prereg\_Rsp* message with a Result code TLV will be sent back to the Target BS). If the Target BS does not support Data Path Pre-Registration and the Anchor ASN-GW attempts to initiate Data Path Pre-Registration procedure, the transaction SHOULD be rejected (i.e., *Path\_Prereg\_Rsp* message with a Result code TLV will be sent back to the Anchor ASN-GW).

The Target BS SHALL respond to the *HO\_Req* message with the *HO\_Rsp* message, and the Serving BS SHALL acknowledge the Handover Preparation transaction completion by sending a *HO\_Ack* message (see Figure 4-77 and Figure 4-78 for the call flow scenarios).

1 In the case Target BS tries and fails to acquire MS security context (AK context) in the HO Preparation Phase, it  
2 SHALL respond with the *HO\_Rsp* message including either the appropriate BS HO RSP Code value or Failure  
3 Indication.

4 The Serving/Anchor and Target ASN-GWs, MAY optionally include the relevant Data Path Info TLVs within the  
5 relevant HO Control messages. In other words the *HO\_Req* message may also include the data path control  
6 information contained in the *Path\_Prereg\_Req* message and the *HO\_Rsp* message may include the information  
7 contained in the *Path\_Prereg\_Rsp* message. The *HO\_Ack* message will also serve as the *Path\_Reg\_Ack* message.

8 The combining or piggybacking of data path pre-registration messages over handover control messages is possible  
9 only when both Anchor ASN-GW and Target BSs support this feature. The Anchor ASN-GW MAY initiate this  
10 procedure, but if the Target BS doesn't support message combining it will simply ignore the Data Path Info TLVs in  
11 the *HO\_Req* message and respond with an *HO\_Rsp* message which doesn't contain any Data Path Info TLVs. In this  
12 case the Target BS MAY initiate Data Path Pre-Registration on its own (i.e., proceed according to the Scenario 2,  
13 shown in Figure 4-78).

14 If the Target BS supports HO Control and DP Control message combining and receives a *HO\_Req* message  
15 combined with *Data Path Info* TLVs, it SHALL respond with the *HO\_Rsp* message combined with *Data Path Info*  
16 TLVs. Consequently, a *HO\_Ack* message SHALL be sent by the Serving BS as the acknowledgment of the *HO\_Rsp*  
17 message.

18 Target BS MAY initiate Data Path Pre-Registration procedure on its own.

19 Upon successful 3-way Path Prereg procedure, Target BS SHALL start the *Path\_Retain* timer. The Path Retain timer  
20 is used to delete pre-registered Data Path in the event the MS does not handover to the Target BS and Data Path  
21 Deregistration is not received from the Anchor ASN-GW.

22 To summarize, data path pre-registration during the handover preparation phase is optional and may occur when  
23 both the Target BS and Anchor ASN-GW support the procedure. The Target BS or Anchor ASN-GW may choose  
24 not to perform data path pre-registration. Retrieval of AK Context from the Authenticator by the Target ASN during  
25 the Handover Preparation phase is also optional and may otherwise occur during the Handover Action phase.

#### 26 **4.7.2.1.1 Handover Preparation Scenario 1: AK Context Retrieval and Path Pre-Registration** 27 **Initiated by Target BS**

28 The following call flow describes a successful inter-ASN handover preparation scenario where the Serving BS  
29 provides the Target BS with the Authenticator ID and the Target BS pre-establishes the data path during the  
30 preparation phase.

31 In the HO Preparation Phase, if Anchor ASN-GW is not collocated with the Serving ASN-GW, the *HO\_Req*  
32 message will not go through Anchor ASN-GW and no data path pre-establishment info can be sent with *HO\_Req* to  
33 the ASN-GW in the Target ASN. So the data path establishment procedure will be initiated by Target BS separately.

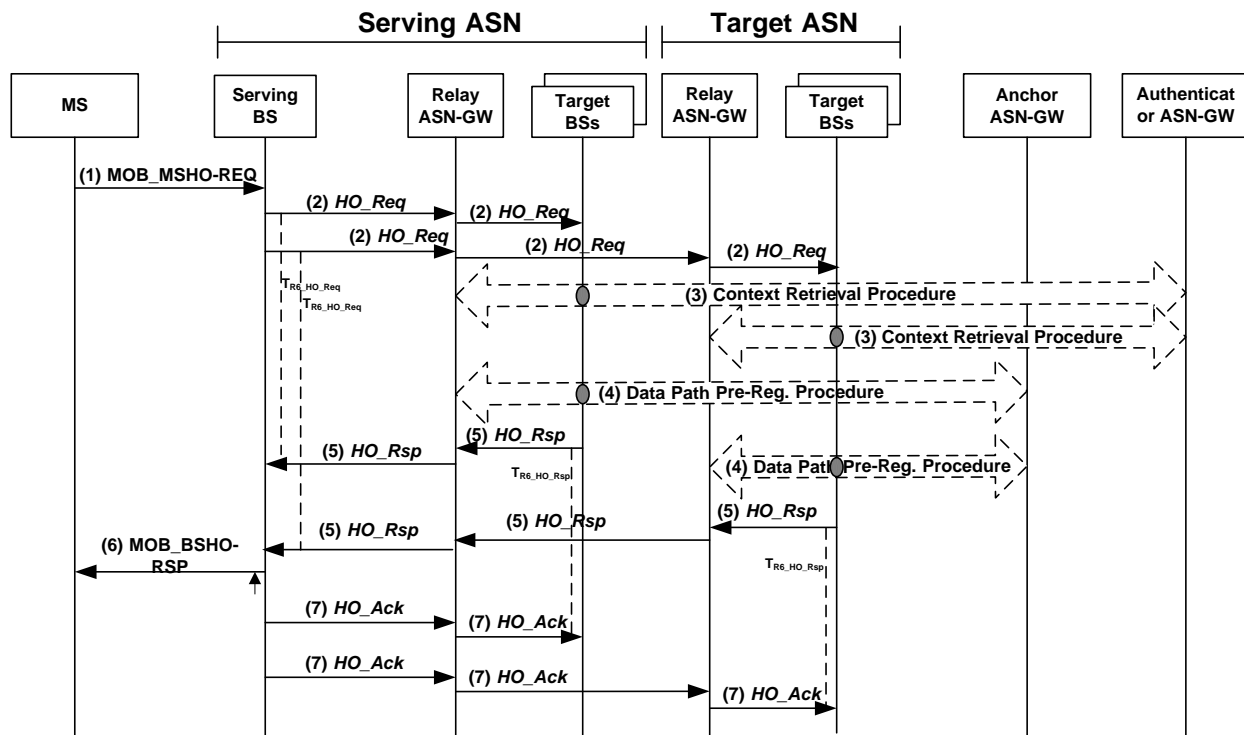


Figure 4-77 – Successful HO Preparation Phase, Scenario 1

### STEP 1

The MS initiates a handover by sending a MOB\_MSHO-REQ message to the Serving BS which includes one or more potential target BS's.

### STEP 2

A Serving BS SHALL silently discard a duplicate MOB\_MSHO-REQ from an MS, if it has already initiated a HO preparation phase for this MS which is still ongoing. If a Serving BS receives such duplicate MOB\_MSHO-REQ from an MS, it SHALL not propagate the request further in to the network.

The Serving BS sends a HO\_Req message for each Target BS selected for the handover via the Serving/Relay ASN-GW and starts timer  $T_{R6\_HO\_Request}$  for each message. The message includes an Authenticator ID TLV that points to the Authenticator/Key Distributor function at the Authenticator ASN-GW and the Anchor ASN GW ID of the Anchor Data Path function at the Anchor ASN-GW.

The Relay ASN-GW relays each HO\_Req message to the corresponding Target BS.

### STEP 3

The Target BS(s) requests AK context for the MS by initiating a Context Request procedure (see section 4.12.2) with the Authenticator ASN-GW. If no Authenticator ID TLV was received (this means Serving ASN-GW is co-located with the Authenticator ASN-GW), the Target BS initiates a Context Retrieval procedure with the Serving ASN-GW. Note: The Target BS(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 BS(s) may initiate pre-establishment of a data path for the MS with the Anchor ASN-GW. It can be initiated if the Serving ASN-GW included the Anchor ASN GW ID in the HO\_Req message by initiating a Data Path Pre-Registration procedure (see section 4.12.1) with the Anchor ASN-GW. If the Anchor ASN GW ID was not included, the Serving ASN-GW hosts the Anchor Data Path function and

the Target BS(s) initiates the Data Path Pre-Registration procedure with the Serving ASN-GW. If the Anchor ASN-GW does not support the Data Path Pre-Registration procedure, the *Path\_Prereg\_Req* message from the Target ASN-GW will be responded by the *Path\_Prereg\_Rsp* message with an appropriate failure indication. Note: The Target BS(s) may optionally choose to defer this procedure to the handover action phase.

#### STEP 5

The Target BS(s) sends a *HO\_Rsp* message to the Serving BS via Relay ASN-GW(s) as a response to *HO\_Req* message and starts  $T_{R6\_HO\_Response}$ . The Relay ASN-GW relays the *HO\_Rsp* messages to the Serving BS. Upon receipt of the *HO\_Rsp* message, the Serving BS stops timer  $T_{R6\_HO\_Req}$ .

In the case Target BS tries and fails to acquire MS security context (AK context) in the step 3, it SHALL respond with the *HO\_Rsp* message including either the appropriate BS HO RSP Code value or Failure Indication

#### STEP 6

The Serving BS sends a MOB\_BSHO-RSP message to the MS containing one or more potential target BS's selected by the network for the MS to handover to.<sup>5</sup>

#### STEP 7

The Serving BS sends a *HO\_Ack* message to the Target BS(s) controlling the potential target BS(s) selected for the MS. Relay ASN-GW relays the message to the Target BS(s). Upon receipt of the *HO\_Ack* message, the Target BS(s) stops timer  $T_{R6\_HO\_Rsp}$ .

#### 4.7.2.1.2 Handover Preparation Scenario 2: AK Context sent by Serving ASN-GW and Path Pre-Registration Initiated by Target ASN-GW

The following call flow describes a successful inter-ASN handover preparation scenario where the Serving ASN-GW is collocated with the Authenticator ASN-GW, and then includes piggybacked information (AK Context) when relaying a handover message to a Target BS. In the scenario, the Target BS pre-establishes the data paths during the preparation phase.

---

<sup>5</sup> 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.

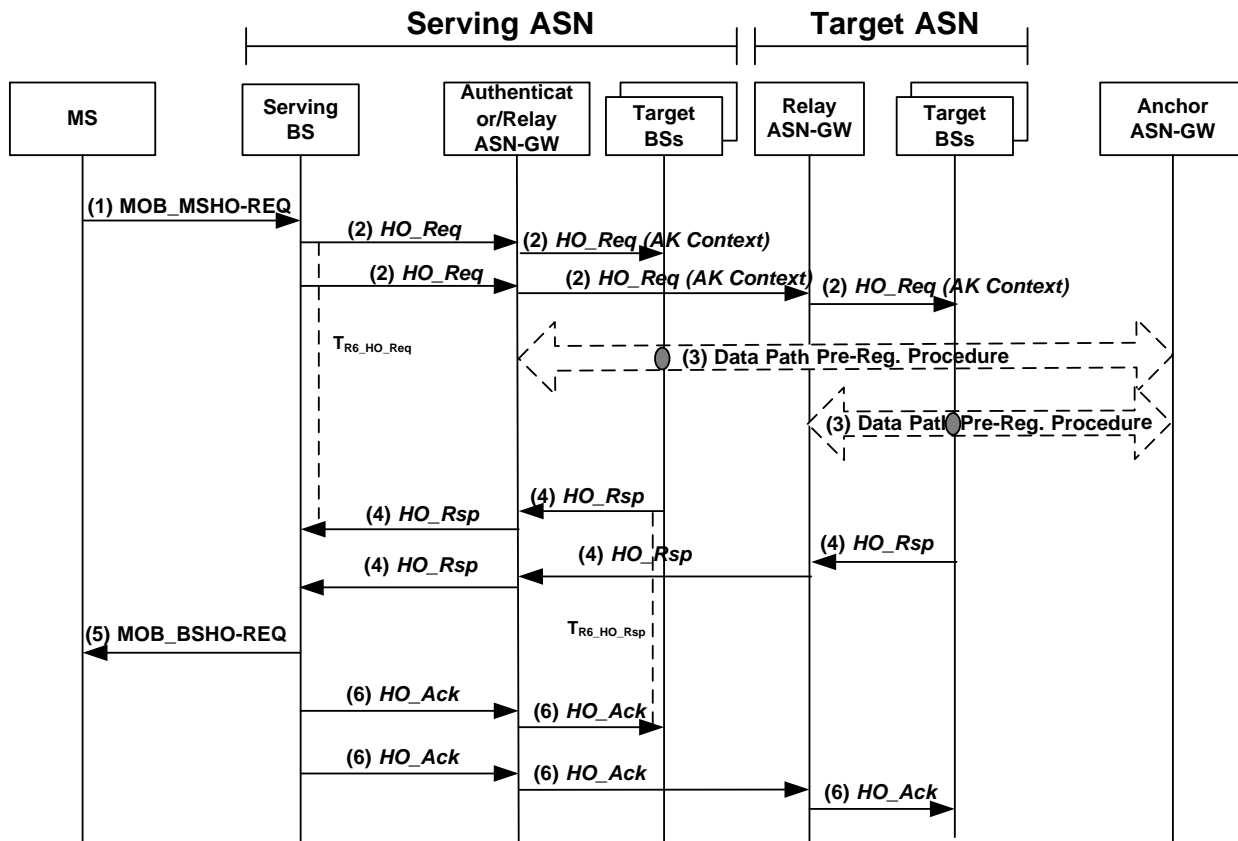


Figure 4-78 – Successful HO Preparation Phase, Scenario 2

### STEP 1

The MS initiates a handover by sending a MOB\_MSHO-REQ message to the Serving BS which includes one or more potential target BS's.

### STEP 2

Serving BS sends *HO\_Req* to one or more Target BS(s) by help of the message relay function in the Serving ASN-GW and starts timer  $T_{R6\_HO\_Req}$ . The message includes the Anchor ASN GW ID and Authenticator ASNGW ID.

The Serving ASN-GW forwards the *HO\_Req* message to the respective Target BS without change except for the following cases: In case where the Serving ASN-GW is collocated with the Authenticator ASN-GW, upon receiving the *HO\_Req* message from the Serving BS, the Serving ASN-GW MAY piggyback the AK context for the MS when sending the *HO\_Req* message to the Target BS. However if AK context is not provided by the MS' Authenticator for usage with the respective Target BS, the Serving ASN-GW forwards the *HO\_Req* message to this Target BS without AK context as Scenario 1

Note: The context retrieval and sending it in the *HO\_Req* message by the Serving ASN-GW in the handover preparation phase is optional and may be deferred to the handover action phase.

### STEP 3

The Target BS pre-establishes a data path for the MS by initiating the Data Path Pre-Registration procedure (see section 4.12) with the Anchor ASN-GW. If the Anchor ASN GW ID was not included, the Serving ASN-GW hosts



the Anchor Data Path function and the Target BS initiates the Data Path Pre-Registration procedure with the Anchor ASN-GW. Note: The Target BS(s) may optionally choose to defer this procedure to the handover action phase.

**STEP 4**

The Target BS sends a *HO\_Rsp* message to the Serving BS to acknowledge the handover request via Relay ASN-GW and starts timer  $T_{R6\_HO\_Rsp}$ . Upon receipt of the *HO\_Rsp* message, the Serving BS stops timer  $T_{R6\_HO\_Req}$ .

**STEP 5**

The Serving BS sends a MOB\_BSHO-RSP message to the MS containing one or more target BS's selected by the network for the MS to handover to<sup>6</sup>.

**STEP 6**

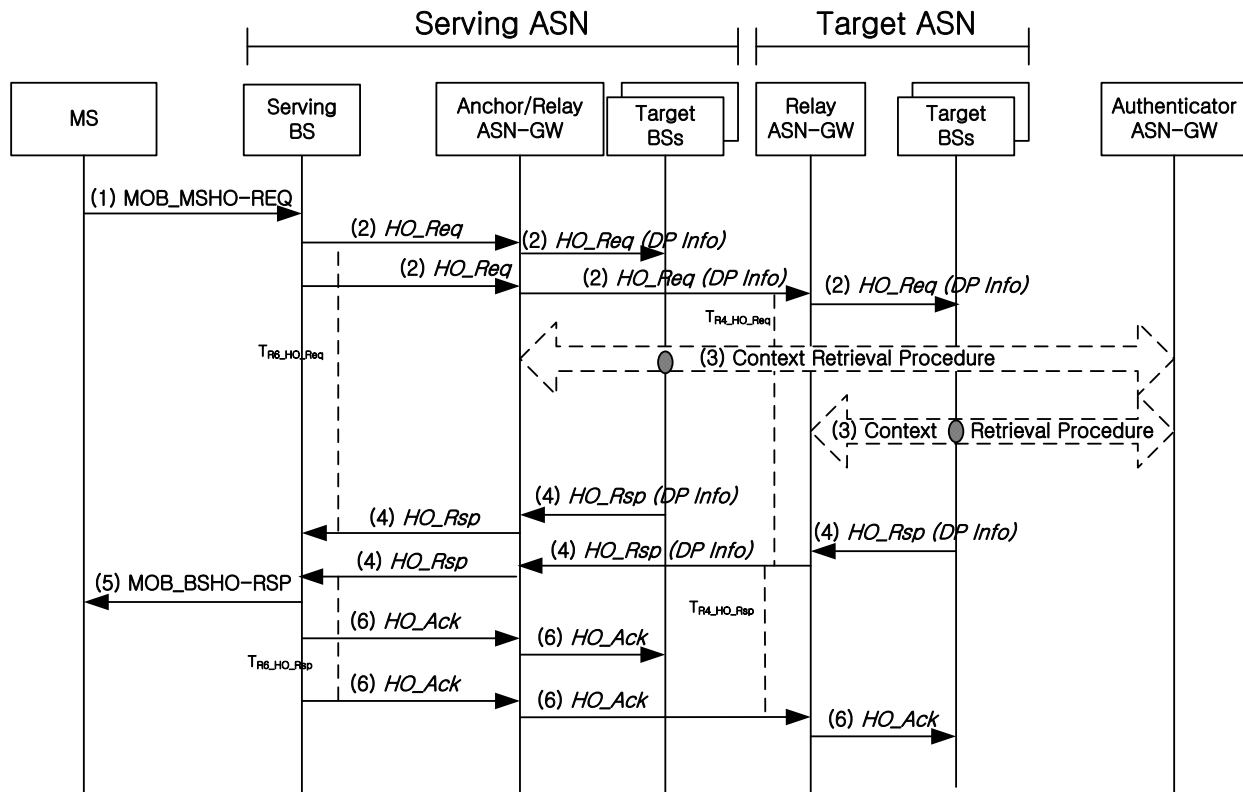
The Serving BS sends a *HO\_Ack* message to the Target BSs selected for the MS via Relay ASN-GW. Upon receipt of the *HO\_Ack* message, the Target BS stops timer  $T_{R6\_HO\_Rsp}$ .

**4.7.2.1.3 Handover Preparation Scenario 3: Anchor ASN-GW Collocated with Serving ASN-GW and Path Pre-Registration Piggybacked onto HO Control messages**

The following call flow describes a successful inter-ASN handover preparation scenario where the Anchor ASN-GW is co-located with the Serving ASN-GW. In this scenario, the Serving/Anchor ASN-GW initiates data path pre-establishment with the Target BS(s) with the piggybacked handover messages. The handover signaling is optimized by “piggybacking” data path pre-registration signaling onto handover control messages.

---

<sup>6</sup> Same note as the Note 1



**Figure 4-79 – Successful HO Preparation Phase, Scenario 3**

### STEP 1

The MS initiates a handover by sending a MOB-MSHO\_REQ message to the Serving BS which includes one or more candidate target BS's.

### STEP 2

In case where the Serving ASN-GW is collocated with the Anchor ASN-GW upon receipt of the HO\_Req message from the Serving BS, the Serving ASN-GW sends an HO\_Req message containing the Data Path Info TLV to the Target BS and starts timer  $T_{R4\_HO\_Req}$ .

### STEP 3

The Target BS(s) requests AK context for the MS by initiating a Context Request procedure (see section 4.12.2) with the Authenticator ASN-GW. If no Authenticator ID TLV was received (this means Serving ASN-GW is collocated with the Authenticator ASN-GW), the Target BS initiates a Context Retrieval procedure with the Serving ASN-GW. Note: The Target BS(s) may optionally choose to defer this procedure to the handover action phase.

If AK context request for the particular Target BS has been rejected by the MS' Authenticator, the Target BS SHALL send HO\_Rsp message with appropriate Failure Indication value to the Serving BS.

### STEP 4

The Target BS responds by sending a HO\_Rsp message which includes the Data Path Info TLV to the Serving ASN to acknowledge the handover request and the piggybacked Data Path Info TLV, and starts timer  $T_{R6\_HO\_Rsp}$ . Upon receipt of the HO\_Rsp message, the Serving ASN stops timer  $T_{R4\_HO\_Req}$ . Note: if the Target BS does not support piggybacking of data path pre-registration signaling onto handover signaling, the Target BS may respond by initiating a data path pre-registration procedure with the Serving/Anchor ASN-GW.

## STEP 5

The Serving BS sends a MOB\_BSHO-RSP message to the MS containing one or more potential target BS's selected by the network for the MS to handover to.

## STEP 6

The Serving BS sends a *HO\_Ack* message to the Target BS(s) selected by the MS. This message also serves as a three-way handshake for the Data Path Pre-Registration. Upon receipt of the *HO\_Ack* message, the Target BS(s) stops timer  $T_{R6\_HO\_Rsp}$ .

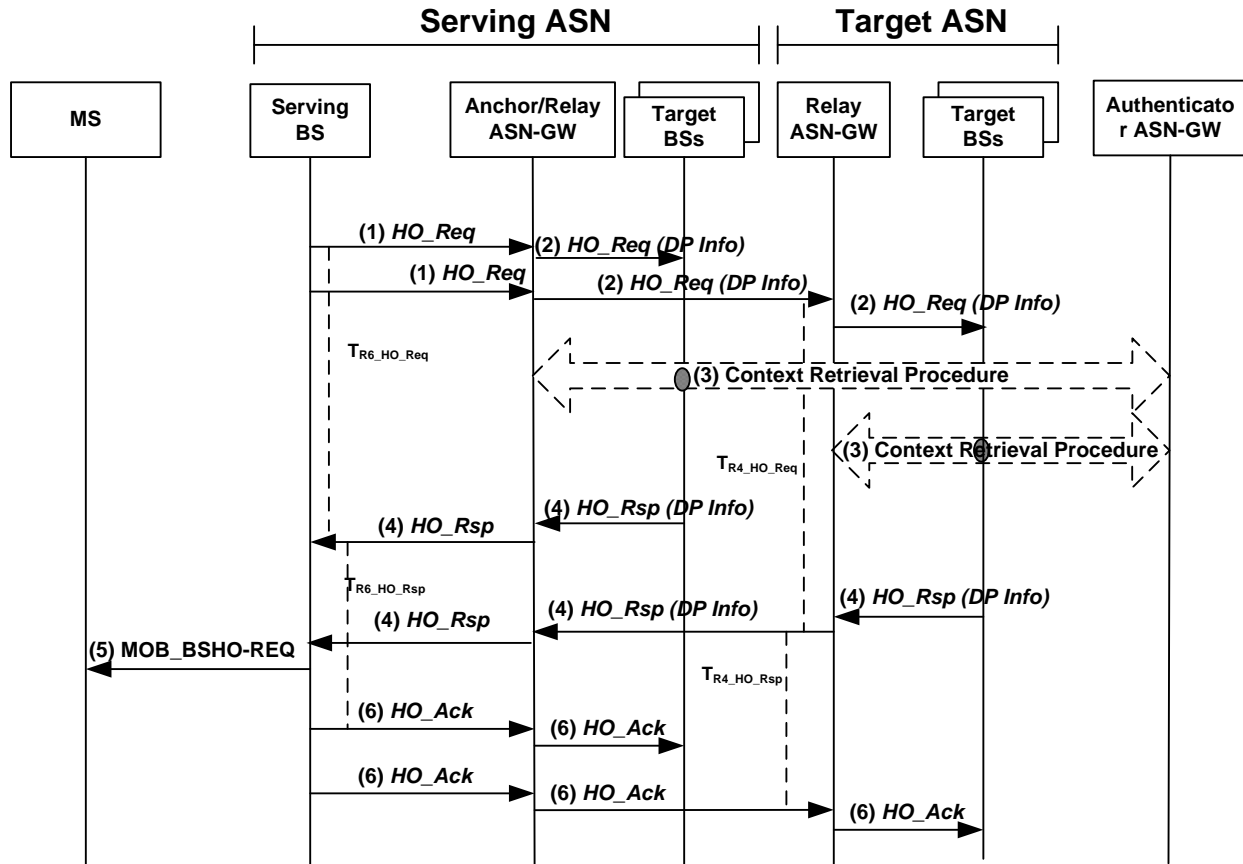


Figure 4-80 – Successful HO Preparation Phase, Scenario 5

## STEP 1

The Serving BS initiates a handover by sending a *HO\_Req* message to each potential target BS selected for the handover and starts timer  $T_{R6\_HO\_Req}$  for each message. The message includes an Authenticator GW ID TLV that points to the Authenticator/Key Distributor function at the Authenticator ASN-GW and the Anchor ASN GW ID of the Anchor Data Path function at the Anchor ASN-GW.

The Serving BS may send the message to multiple Target BS's for the potential handover.

## STEP 2

In case where the Serving ASN-GW is collocated with the Anchor ASN-GW, upon receipt of the *HO\_Req* message from the Serving BS, the Serving ASN-GW appends a *HO\_Req* message with Data Path Info TLV to the Target BS.

**STEP 3**

The Target BS(s) requests AK context for the MS by initiating a Context Request procedure (see section 4.12.2) with the Authenticator ASN-GW. If no Authenticator ID TLV was received (this means Serving ASN-GW is co-located with the Authenticator ASN-GW), the Target BS initiates a Context Retrieval procedure with the Serving ASN-GW. Note: The Target BS(s) may optionally choose to defer this procedure to the handover action phase.

If AK context request for the particular Target BS has been rejected by the MS' Authenticator, the Target BS SHALL reject the handover request by sending *HO\_Rsp* message with appropriate Failure Indication value to the Serving BS.

**STEP 4**

The Target BS responds by sending a *HO\_Rsp* message which includes the Data Path Info TLV to the Serving ASN-GW to acknowledge the handover request and the piggybacked Data Path Info TLV, and starts timer  $T_{R6\_HO\_Rsp}$ . Upon receipt of the *HO\_Rsp* message, the Serving ASN-GW stops timer  $T_{R4\_HO\_Req}$ . Note: if the Target BS does not support piggy backing of data path pre-registration signaling onto handover signaling, the Target BS may respond by initiating a Data Path Pre-Registration procedure with the Serving/Anchor ASN-GW.

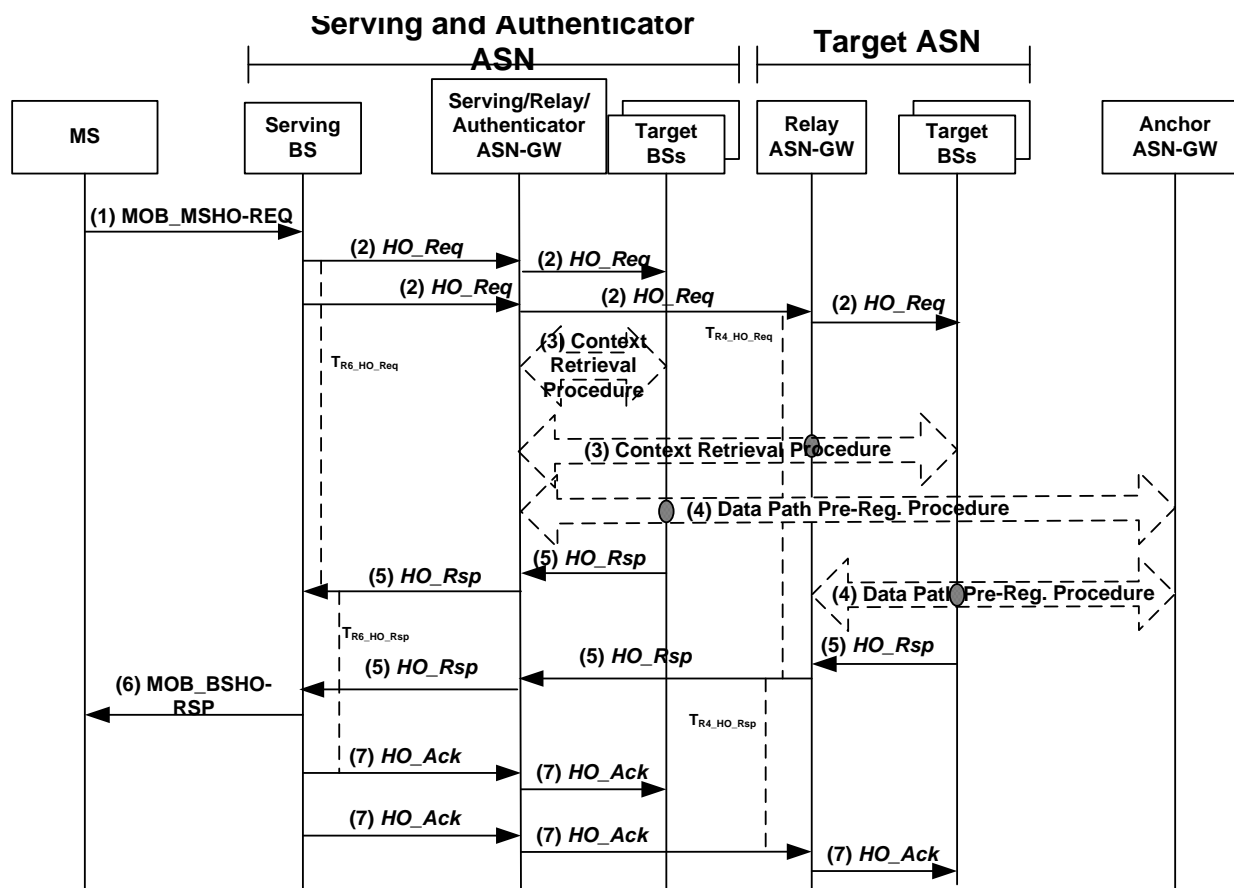
**STEP 5**

The Serving BS sends a MOB\_BSHO-REQ message to the MS containing one or more potential target BS's selected by the network for the MS to handover to.

**STEP 6**

The Serving BS sends a *HO\_Ack* message to the Target BS(s) selected by the MS via Relay ASN-GW. This message also serves as a three-way handshake for the data path pre-registration. Upon receipt of the *HO\_Ack* message, the Target BS(s) stops timer  $T_{R6\_HO\_Rsp}$ .

#### 4.7.2.1.4 MS-Initiated HO Preparation Phase – Co-located Serving, Relay and Authenticator ASN-GW (Scenario 6)



**Figure 4-81 – Successful HO Preparation Phase (The Serving, Relay and the Authenticator ASN-GW are collocated)**

##### STEP 1

The MS initiates a handover by sending a MOB-MSHO\_REQ message to the Serving BS which includes one or more candidate target BS's.

##### STEP 2

The Serving BS sends a *HO\_Req* message to each potential target BS selected for the handover and starts timer  $T_{R6\_HO\_Req}$  for each message. The message includes an Authenticator GW ID TLV that points to the Authenticator/Key Distributor function at the Authenticator ASN-GW and the Anchor ASN GW ID of the Anchor Data Path function.

A Serving BS SHALL silently discard a duplicate MOB\_MSHO-REQ from an MS, if it has already initiated a HO preparation phase for this MS which is still ongoing. If a Serving BS receives such duplicate MOB\_MSHO-REQ from an MS, it SHALL not propagate the request further in to the network.

The Serving BS sends a *HO\_Req* message to the Target BS where the Serving BS starts timer  $T_{R6\_HO\_Req}$  and the Target Relay ASN-GW starts  $T_{R4\_HO\_Req}$ . The Serving BS may send the message to multiple Target BS's for the potential handover. The Relay ASN-GW relays each *HO\_Req* message to the corresponding Target BS.

**STEP 3**

The Target BS(s) requests AK context for the MS by initiating a Context Request procedure (see section 4.12.2) with the Authenticator ASN-GW (Serving ASN-GW is co-located with the Authenticator ASN-GW). The Relay GW relays the message. Note: The Target BS(s) may choose to defer this procedure to the handover action phase.

**STEP 4**

The Target BS(s) may initiate pre-establishment of a data path for the MS with the Anchor ASN-GW after receiving *HO\_Req* message. If the Anchor ASN-GW does not support the Data Path Pre-Registration, the R6 *Path\_Prereg\_Req* message from the Target BS will be responded by the R6 *Path\_Prereg\_Rsp* message with an appropriate failure indication. It can be initiated, if the Serving ASN-GW included the Anchor ASN GW ID TLV in the *HO\_Req* message, by initiating a Data Path Pre-Registration procedure (see section 4.12.1) with the Anchor ASN-GW. If the Anchor ASN GW ID TLV was not included, the Serving ASN-GW also hosts the Anchor Data Path function and the Target ASN-GW(s) initiates the Data Path Pre-Registration procedure with the Serving ASN-GW. Note: The Target BS(s) MAY choose to defer this procedure to the handover action phase.

**STEP 5**

The Target BS(s) sends a *HO\_Rsp* message to the Serving BS to acknowledge the handover request where Serving BS starts timer  $T_{R6\_HO\_Rsp}$ . The Relay ASN-GW relays the *HO\_Rsp* messages to the Serving BS and starts  $T_{R4\_HO\_Rsp}$ . Upon receipt of the *HO\_Rsp* message, the Serving BS stops timer  $T_{R6\_HO\_Req}$ .

In the case Target BS tries and fails to acquire MS security context (AK context) in the HO Preparation Phase, it responds with the *HO\_Rsp* message including either the appropriate BS HO RSP Code value or Failure Indication.

**STEP 6**

The Serving BS sends a MOB\_BSHO-RSP message to the MS containing one or more potential target BS's selected by the network for the MS to handover.

**STEP 7**

The Serving BS sends a *HO\_Ack* message to the Target BS(s), selected for the MS. The Relay ASN-GW relays the *HO\_Ack* message(s) to the corresponding Target BS(s). Upon receipt of the *HO\_Ack* message, the Target BS(s) stops timer  $T_{R6\_HO\_Rsp}$ .

**4.7.2.1.5 Network Initiated HO Scenarios**

Network Initiated Handover message transactions associated with the Network Initiated HO Preparation Phase are identical to the transactions associated with the MS Initiated HO Preparation Phase. The difference is in the air interface transactions. Handover is triggered by the internal logic in the Serving ASN (or Serving/Anchor ASN if collocated), without receiving any handover related messages initiated by the MS. The Network Initiated HO Preparation Phase ends with sending MOB\_BSHO-REQ to the MS.

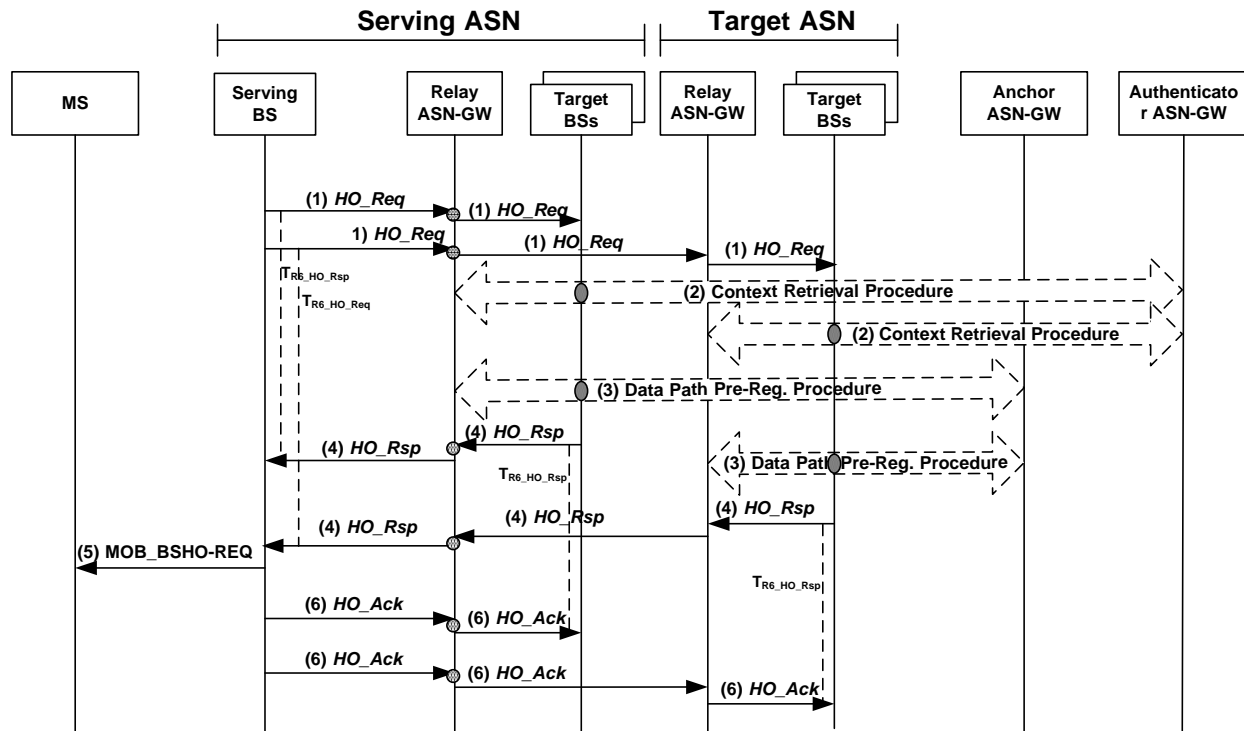


Figure 4-82 – Successful HO Preparation Phase (Network Initiated)

### STEP 1

The Serving BS sends a *HO\_Req* message to one or more Target BS's selected for the handover and starts timer  $T_{R6\_HO\_Req}$  for each message. The message includes an Authenticator ID TLV that points to the Authenticator/Key Distributor function at the Authenticator ASN-GW and the Anchor ASN GW ID TLV. The Relay ASN-GW relays the *HO\_Req* messages to the corresponding Target BS.

### STEP 2

The Target BS(s) requests AK context for the MS by initiating a Context Request procedure (see section 4.12) with the Authenticator ASN-GW. If no Authenticator ID was received (Serving ASN-GW is co-located with the Authenticator ASN-GW), the Target BS initiates a Context Request procedure with the Serving ASN-GW.

Note: The Target BS(s) may optionally choose to defer this procedure to the handover action phase.

### STEP 3

The Target BS(s) may initiate pre-establishment of a data path for the MS with the Anchor ASN after receiving *HO\_Req* message. It can be initiated, if the Serving BS included the Anchor ASN GW ID TLV in the *HO\_Req* message, by initiating a Data Path Pre-Registration procedure (see section 4.12) with the Anchor ASN-GW. If the Anchor ASN GW ID TLV was not included, the Serving ASN-GW hosts the Anchor Data Path function and the Target BS(s) initiates the Data Path Pre-Registration procedure with the Serving ASN-GW. If the Anchor ASN-GW does not support the Data Path Pre-Registration, the *Path\_Prereg\_Req* message from the Target BS will be responded by the *Path\_Prereg\_Rsp* message with an appropriate failure indication.

Note: The Target BS(s) may optionally choose to defer this procedure to the handover action phase.

#### STEP 4

The Target BS(s) sends a *HO\_Rsp* message to the Serving BS to acknowledge the handover request. Relay ASN-GW relays the message to the Serving BS where the Target Relay ASN-GW starts timer  $T_{R4\_HO\_Rsp}$ . Upon receipt of the *HO\_Rsp* message, the Serving ASN stops timer  $T_{R6\_HO\_Req}$  and starts timer  $T_{R6\_HO\_Rsp}$ .

In the case Target ASN tries and fails to acquire MS security context (AK context) in the HO Preparation Phase, it responds with the *HO\_Rsp* message including either the appropriate BS HO RSP Code value or Failure Indication.

#### STEP 5

The Serving BS sends a *MOB\_BSHO-REQ* message to the MS with the Mode TLV set to 0b000 (HO Request) and containing one or more potential target BS's selected by the network for the MS to handover to. See IEEE 802.16e section 6.3.2.3.52.

#### STEP 6

The Serving BS sends a *HO\_Ack* message to the Target BS(s) selected for the MS. The Relay ASN-GW relays the R6 *HO\_Ack* message(s) to the corresponding Target BS(s). Upon receipt of the *HO\_Ack* message, the Target BS(s) stops timer  $T_{R6\_HO\_Rsp}$ .

Figure 4-80 shows a Network Initiated HO Preparation scenario which, from the network point of view, is identical to scenario 4 discussed in subclause 4.7.2.1.3.

#### 4.7.2.1.6 HO Preparation Stage Timers and Timing Considerations

This section identifies the timer entities participating in the HO Preparation Phase. The following timers are defined over R6:

- $TR6\_Path\_Pre\_Req$ : is started by the BS initiating pre-registration 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.
- $TR6\_Path\_Pre\_Rsp$ : is started by the Anchor ASN-GW responding to pre-establishment of the data path for an MS, upon sending the R6 *Path\_Prereg\_Rsp* message and is stopped upon receiving a corresponding R6 *Path\_Prereg\_Ack* message.
- $TR6\_Cntxt\_Req$ : is started by the BS requesting context for a specific MS, upon sending the R6 *Context\_Req* message and is stopped upon receiving a corresponding R6 *Context\_Rpt* message.
- $TR6\_HO\_Req$ : is started by a Serving BS upon sending the R6 *HO\_Req* message for an MS to a Target BS and is stopped upon receiving a corresponding R6 *HO\_Rsp* message from the Target BS.
- $TR6\_HO\_Rsp$ : is started by a Target BS upon sending the R6 *HO\_Rsp* message for an MS to a Serving BS and is stopped upon receiving a corresponding R6 *HO\_Ack* message from the Serving BS.

The following timers are defined over R4:

- $T_{R4\_Path\_Pre\_Req}$ : is started by the ASN-GW initiating pre-establishment of the data path for an MS, upon sending the R4 *Path\_Prereg\_Req* message and is stopped upon receiving a corresponding R4 *Path\_Prereg\_Rsp* message.
- $T_{R4\_Path\_Pre\_Rsp}$ : is started by the ASN-GW responding to pre-establishment of the data path for an MS, upon sending the R4 *Path\_Prereg\_Rsp* message and is stopped upon receiving a corresponding R4 *Path\_Prereg\_Ack* message.
- $T_{R4\_Cntxt\_Req}$ : is started by the ASN-GW requesting context for a specific MS, upon sending the R4 *Context\_Req* message and is stopped upon receiving a corresponding R4 *Context\_Rpt* message.
- $T_{R4\_HO\_Req}$ : is started by a Serving ASN-GW upon sending the R4 *HO\_Req* message for an MS to a Target ASN-GW and is stopped upon receiving a corresponding R4 *HO\_Rsp* message from the Target ASN.



- $T_{R4\_HO\_Rsp}$ : is started by a Target ASN-GW upon sending the R4 *HO\_Rsp* message for an MS to a Serving ASN-GW and is stopped upon receiving a corresponding R4 *HO\_Ack* message from the Serving ASN.

Table 4-78 shows the default value of timers and also indicates the range of the recommended duration of these timers. Note that these values are provisioned in the current Release.

**Table 4-78 – HO Preparation Phase Timer Values for R4**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R6\_Path\_Pre\_Req}$	TBD		TBD
$T_{R6\_Path\_Pre\_Rsp}$	TBD		TBD
$T_{R6\_Cntxt\_Req}$	TBD		TBD
$T_{R6\_HO\_Req}$	TBD		TBD
$T_{R6\_HO\_Rsp}$	TBD		TBD
$T_{R4\_Path\_Pre\_Req}$	TBD		TBD
$T_{R4\_Path\_Pre\_Rsp}$	TBD		TBD
$T_{R4\_Cntxt\_Req}$	TBD		TBD
$T_{R4\_HO\_Req}$	TBD		TBD
$T_{R4\_HO\_Rsp}$	TBD		TBD

#### 4.7.2.1.7 HO Preparation Stage Error Conditions

This section describes error conditions associated with the HO Preparation Phase.

##### 4.7.2.1.7.1 Timer Expiry

Table 4-79 shows details on 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 4-79.

**Table 4-79 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R6\_Path\_Pre\_Req}$	BS initiating Path Pre-Registration procedure	No action required
$T_{R6\_Path\_Pre\_Rsp}$	ASN-GW responding to <i>Path_Prereg_Req</i> 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
$T_{R4\_Path\_Pre\_Req}$	ASN initiating Data Path Pre-Registration procedure	No action required.

T <sub>R4_Path_Pre_Rsp</sub>	ASN responding to <i>Path_Prereg_Req</i> message	No action required.
T <sub>R4_Cntxt_Req</sub>	ASN Requesting context info	No action required.
T <sub>R4_HO_Req</sub>	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 <sub>R4_HO_Rsp</sub>	Target ASN	No action required.

#### 4.7.2.1.7.2 Context\_Rpt Error

Upon receipt of the *Context\_Req* message, if the ASN-GW is unable to provide the requested information it SHALL send a *Context\_Rpt* message to the sender of the *Context\_Req* message. The *Context\_Rpt* message SHALL include the Failure Indication TLV. Upon receipt of the *Context\_Rpt* message with Failure Indication TLV, the ASN-GW or BS SHALL stop timer T<sub>R4\_Cntxt\_Req</sub> or T<sub>R6\_Cntxt\_Req</sub> (if running) respectively. If the *Context\_Req* message was triggered by the Serving ASN, then upon receipt of the *Context\_Rpt* message with Failure Indication TLV, the Serving BS MAY resend the *Context\_Req* message. If the Serving BS does not resend the *Context\_Req* message or if the subsequent attempts are also unsuccessful, then in the case of MS initiated handover, the Serving BS SHALL send a MOB\_BSHO\_RSP with mode = 0b111 to the MS. If the *Context\_Req* message was triggered by the Target BS, then upon receipt of the *Context\_Rpt* message with Failure Indication TLV, the Target BS MAY resend the *Context\_Req* message. If the Target BS does not resend the *Context\_Req* message or if subsequent attempts are also unsuccessful, then the Target BS SHALL send a *HO\_Rsp* message with suitable error code included in the Result Code TLV.

#### 4.7.2.1.7.3 HO\_Rsp Error

Upon receipt of the *HO\_Req* message, if the Target BS is unable to support the HO, then it SHALL send *HO\_Rsp* message with suitable error code included in the Result Code TLV. Upon receipt of the *HO\_Rsp* message indicating HO cannot be supported, the Serving BS SHALL stop T<sub>R6-HO\_Request</sub> (if running). The Serving BS MAY re-send the *HO\_Req* message to a different Target BS. If the Serving BS does not re-send the *HO\_Req* message, or if all subsequent Target BSs cannot support the HO, in the case of MS Initiated handover, the Serving BS SHALL send a MOB\_BSHO\_RSP with mode = 0b111 to the MS.

#### 4.7.2.1.7.4 Path\_Prereg\_Rsp Error

Upon receipt of the *Path\_Prereg\_Req* message, if the ASN-GW is unable to support the pre-establishment of a data path, then it SHALL send a *Path\_Prereg\_Rsp* message with suitable error code.

Upon receipt of the *Path\_Prereg\_Rsp* message with suitable error code, the ASN-GW SHALL stop T<sub>R4-DP\_Pre-Req</sub> and the BS SHALL stop T<sub>R6-DP\_Pre-Req</sub> (if running) after the R6 *Path\_Rsp* is received.

### 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 MOB\_HO-IND message is the last message the MS sends to the Serving BS. After sending MOB\_HO-IND the MS starts ranging at the selected 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 BS SHALL generate an *HO\_Cnf* message and send it to the Target BS as shown in Figure 4-83. The *HO\_Cnf* message includes the “most recent MAC context” at the Serving BS. The Target BS SHALL complete the 2-way transaction by sending the *HO\_Ack* to the Serving BS.

1 Upon receiving *HO\_Cnf* message with the value for the *HO\_Indication* type which is not set to “Cancel”, the Target  
2 BS MAY retrieve the AK Context if this information was not retrieved or delivered during the Handover Preparation  
3 Phase. This call flow scenario (subsequently referred to as Scenario 1) is shown in Figure 4-83.

4 If the data path between the Anchor ASN-GW and the Target BS was not pre-established at the Preparation Phase, it  
5 MAY be pre-established after receiving *HO\_Cnf* message and before the MS completes Network Re-Entry at the  
6 Target BS. In this case the Target BS initiates Data Path Pre-Registration. The Target BS can expect R4/R6  
7 *Path\_Prereg\_Req* message from the Serving/Anchor ASN. *Path\_Prereg\_Req* and Response message may include  
8 Data Delivery Trigger TLV in the SF Info. If this TLV is included it triggers immediate delivery of data for the  
9 specified Service Flow.

10 The data paths between the Anchor ASN-GW and the Target BS SHALL be established via Data Path Registration  
11 procedure after the MS arrives at the Target BS. The instance of “MS arrival” at the Target BS could be marked by a  
12 mobile initiated ranging, Network Entry completion or Network Re-Entry<sup>7</sup>.

13 If Data Path Registration procedure is invoked after the data path had been pre-registered, the procedure only  
14 confirms final establishment of the pre-registered data paths and does not convey any parameters of the data paths  
15 except MSID. In such case a two-way Data Path Registration handshake will follow since the Data-Path Pre-  
16 registration process had been completed. All the parameters that are related to the data paths SHALL be exchanged  
17 during the preceding Data Path Pre-Registration transaction. Furthermore, the Data Path Registration transaction is  
18 completed with a two-way handshake; *Path\_Reg\_Req* and *Path\_Reg\_Rsp* message exchange and no *Path\_Reg\_Ack*  
19 message (i.e., two-way handshake).

20 If no Data Path Pre-Registration procedure had been completed prior to the Data Path Registration procedure, the R4  
21 *Path\_Reg\_Req* and *Path\_Reg\_Rsp* messages SHALL convey all parameters relevant for the setup of Data Paths. In  
22 this case the R4 *Path\_Reg\_Ack* message SHALL be sent in response to R4 *Path\_Reg\_Rsp* message (i.e., three-way  
23 handshake).

24 After the HO completion, any SFs that have failed in establishing a data path SHALL be regarded as dropped and  
25 SHALL be released by the Anchor ASN-GW.

26 Upon completion of Data Path Registration procedure, the Anchor ASN-GW SHALL initiate de-registration of all  
27 the pre-registered data paths to the candidate Target BSs that have not been selected for the final handover target.  
28 Also, the Anchor ASN-GW MAY initiate de-registration of the data path between itself and the (old) Serving BS.

29 If the Serving BS determines that the *MOB\_HO\_IND* message was not received from the MS due to a  
30 communication loss with the mobile<sup>8</sup> for example upon expiration of an internal timer<sup>9</sup>, the Serving BS may send an  
31 *HO\_Cnf* message (value for the *HO\_Indication* type TLV should be set to a “Unconfirmed”- and latest MAC  
32 context from the MS) to target BSs the MS may chose to handover to via Relay ASN-GW. The *HO\_Cnf* message  
33 may be sent to target BS(s) included in the *MOB\_BSHO-REQ* or *MOB\_BSHO-RSP* messages. The *HO\_Cnf*  
34 message may also be sent to target BSs which were not notified of a potential impending handover from the MS  
35 during the handover preparation phase and whose target BSs were not included in the *MOB\_BSHO-REQ* or  
36 *MOB\_BSHO-RSP* messages. The *HO\_Cnf* message includes the *HO\_Indication* Type TLV set to “Unconfirmed”  
37 and latest MAC context for the MS. When sent to target BSs which weren’t previously notified of an impending  
38 handover from the MS during the handover preparation phase, the *HO\_Cnf* message SHALL also include the  
39 Authenticator GW-ID or AK context, and Anchor GW ID information. Upon sending the *HO\_Cnf* message to the  
40 candidate Target BS(s), the Serving BS SHALL stop all the downlink and uplink scheduling for the data  
41 transmission and reception from the MS respectively.

42 Upon sending the *HO\_Cnf* message, if the *Resource\_Retain* flag was not set, the Serving BS SHALL discard all  
43 MS’s connections resource information including the MAC state machine and all outstanding buffered PDUs, else

---

<sup>7</sup> 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.

<sup>8</sup> *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.

<sup>9</sup> For example, *T<sub>MOB\_HO\_IND</sub>*.

the Serving BS SHALL retain the connections, MAC state machine and PDUs associated with the MS for service continuation until the expiration of Resource Retain Timer.

The Serving BS SHALL release all MAC context and MAC PDUs associated with the MS upon reception of a *HO\_Complete* message from the Target ASN indicating MS completed a Network re-entry at the Target BS.

The *HO\_Cnf* message may be delayed in the backbone network and arrive after the MS completes Network Re-Entry. If the R4 *HO\_Cnf* message is not received by the Target BS until the MS appears at the Target BS, the Target BS MAY request the “most recent MAC Context” via *Context\_Req* and *Context\_Rpt* exchange with the Serving ASN as it is shown in Scenario 2.

After obtaining all the necessary MS Context, the Target BS SHALL perform the Data Path Registration procedure.

Immediately after the MS completes network re-entry, the Target ASN (which at that moment becomes new Serving ASN) SHALL update the Authenticator ASN-GW about successful HO completion via *CMAC\_Key\_Count\_Update*. *CMAC\_Key\_Count\_Update* message SHALL deliver to the Authenticator the value of the *CMAC\_KEY\_COUNT* the Target ASN holds. Normally this value will be identical to the one the Target BS received with *Context\_Rpt* from the Authenticator BS. However if the Target BS in the Target ASN receives and authenticates an RNG-REQ message containing a *CMAC\_KEY\_COUNT* higher than its own, it SHALL adopt the received count. The resulting count SHALL be delivered to the Authenticator ASN-GW. For details of *CMAC Key Count Update*, refer to section 4.3.4.2. As soon as the MS Network Re-entry procedure at the Target BS is completed, the Target BS SHALL send a *HO\_Complete* message to the Serving BS to provide an accurate HO indication and expedite the resource release in the Serving BS. The Serving BS SHALL complete the 2-way transaction by sending the *HO\_Ack*. Upon receiving the *HO\_Complete* message, if the Serving BS did not yet release resources at the unselected target BS(s), the Serving BS SHALL release the resources at the unselected target BSs by sending the *HO\_Cnf* message with Cancel indication. At this point the Serving BS SHOULD initiate Data Path De-registration procedure with the Anchor BS unless the de-registration procedure has already been initiated by the Anchor ASN.

If the target BS can't retrieve the necessary context due to error code "no record found" from serving BS or authenticator ASN-GW, it SHALL notify MS to conduct full network re-entry.

The *HO\_Cnf* message with ‘cancel’ type may be sent to all candidate target BSs that were not selected as a target for handover. The candidate BSs may initiate the DP release procedure. After receiving this message if they have completed the Path Prereg procedure during the Handover Preparation phase.

Unselected candidate target BS SHALL initiate Path Deregistration process if the Path Retain timer associated with the Path Deregistration expires and the Path Deregistration request has not been received from the Anchor ASN-GW.

If the MS rejects the target BS(s) offered by the serving BS in the *MOB\_BSHO-RSP* (MS initiated handover) or *MOB\_BSHO-REQ* (network initiated handover) message for the MS to handover to by sending a *MOB\_HO-IND* message with *HO\_IND\_type* TLV set to 0b10 to the serving BS, the serving BS notifies the candidate Target BS previously notified of a potential handover from the MS in the handover preparation phase by sending an *HO Confirm* message with a cancellation indication.

If the serving BS offers a new target BS candidate for the MS to handover to, it first notifies the Target BS(s) of a potential handover from the MS as described in the handover preparation scenarios in section 4.7.2.1 via the Relay ASN-GW, then resends the *MOB\_BSHO-RSP* (if MS initiated handover described in section 4.7.2.1.4) or *MOB\_BSHO-REQ* (if network initiated handover described in section 4.7.2.1.5) message containing the new target BS offered to the MS for handover.

The MS may be forced to perform a handover by sending a *MOB\_HO-IND* message with *HO\_IND\_type* set to 0b00 (Serving BS release) but including a preferred Target BS which was not offered by the Serving BS in the *MOB\_BSHO-RSP* or *MOB\_BSHO-REQ* message for the MS to handover to. This case is handled in the handover action scenario 1 below, together with the normal, fully prepared handover case.

#### **4.7.2.2.1 Handover Action Scenario 1: Serving BS Sends *HO\_Cnf* to Target BS**

The following call flow describes a successful inter-ASN handover action scenario where the Target BS receives the *HO\_Cnf* message from the Serving BS, and the Serving BS receives *MOB\_HO-IND* and sends the *HO\_Cnf* message to the Target BS (via Relay ASN-GW). The call flow also addresses the case where the target BS receives the

- 1 HO\_Cnf message from the Serving BS but the target BS was not notified of a potential impending handover from
- 2 the MS during the handover preparation phase and its target BSs were not included in the MOB\_BSHO-REQ or
- 3 MOB\_BSHO-RSP messages.

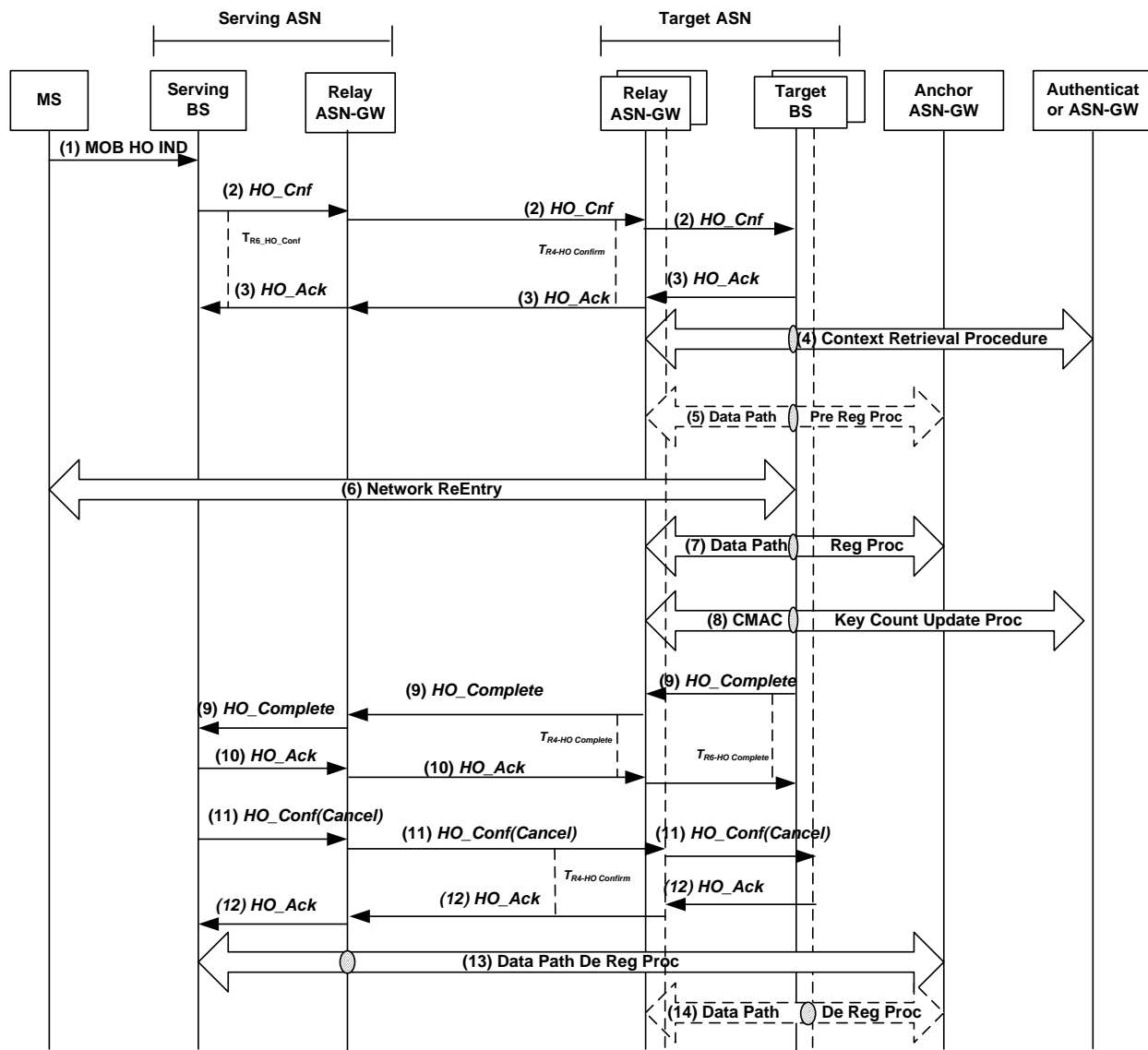


Figure 4-83 – Successful HO Action Phase, Scenario 1

## STEP 1

The MS sends a MOB\_HO-IND to the Serving BS to initiate a handover to one of the target BSs proposed or selected by the Serving BS in the Handover Preparation phase or potentially, in line with [13], to a target BS which has not been proposed by the Serving ASN-GW in the Handover Preparation phase.

## STEP 2

Upon reception of the MOB\_HO-IND the Serving BS sends a HO\_Cnf message to the selected Target BS and starts timer  $T_{R6\_HO\_Conf}$ . The Serving BS MAY also send HO\_Cnf message with the value of the HO\_Indication type set to “Cancel” to all unselected Target BS(s) and clear the MS context anytime after receiving MOB\_HO-IND message. – In case that the selected Target BS was not notified of a potential impending handover from the MS during the

handover preparation phase and its target BSs where not included in the MOB\_BSHO-REQ or MOB\_BSHO-RSP messages, the *HO\_Cnf* message SHALL also include the Authenticator GW-ID or AK context, and Anchor GW ID (Anchor ASN-GW) information.

Relay ASN-GW relays the *HO\_Cnf* message over R6/R4.

### STEP 3

The Target BS sends a *HO\_Ack* message to the Serving BS. Relay ASN-GW relays the *HO\_Ack* message over R4/R6. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Conf}$ .

### STEP 4

If an Authenticator ID TLV was included in the *HO\_Req* or *HO\_Cnf* message and AK context for the MS was not requested during the Handover Preparation phase, the Target BS requests AK context for the MS by initiating a Context Request procedure (see section 4.12.2) with the Authenticator ASN-GW.

### STEP 5

If the Anchor ASN GW ID TLV was included in the *HO\_Req* or *HO\_Cnf* message and Data Path Pre-Registration procedure (see section 4.12.1) did not occur, the Data Path Pre-Registration procedure may optionally take place at this moment.

### STEP 6

The MS initiates network re-entry with the Target BS by sending RNG-REQ.

The Target BS responds with RNG-RSP and the MS and the Target BS complete Network Reentry..

### STEP 7

Target BS initiates Data Path Registration procedure (see section 4.12.3) with the Anchor ASN. Note: This procedure SHALL be a two-way handshake if data path was pre-established.

This procedure MAY take place immediately after Step 4.

### STEP 8

Upon successful completion of network re-entry, Target BS initiates CMAC Key Count Update procedure (see section 4.12.5) and updates the Authenticator ASN-GW with the latest CMAC Key Count value received from MS.

### STEP 9

Upon completion of network re-entry, the Target BS SHALL send a *HO\_Complete* message to the Serving BS to notify the completion of the handover and starts the timer  $T_{R6\_HO\_Comp}$ . Relay ASN-GW relays the *HO\_Complete* message over R6/R4 to the Serving BS. Upon receipt of the *HO\_Complete* message, the Serving BS releases the MS context.

### STEP 10

The Serving BS sends a *HO\_Ack* message to the Target BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Comp}$ .

### STEP 11

Upon receiving the *HO\_Complete* message, if Serving BS did not send *HO\_Cnf* message with the value of the *HO\_Indication* type set to “Cancel” to all unselected Target BS(s) in STEP 2, it SHALL send an *HO\_Cnf* message with the value of the *HO\_Indication* type set to “Cancel” to all unselected Target BS(s) to clear the MS context and starts timer  $T_{R6\_HO\_Conf}$ .

Relay ASN-GW relays the *HO\_Cnf(Cancel)* message over R6/R4.

**STEP 12**

The unselected Target BS sends a *HO\_Ack* message to the Serving BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Conf}$ .

**STEP 13**

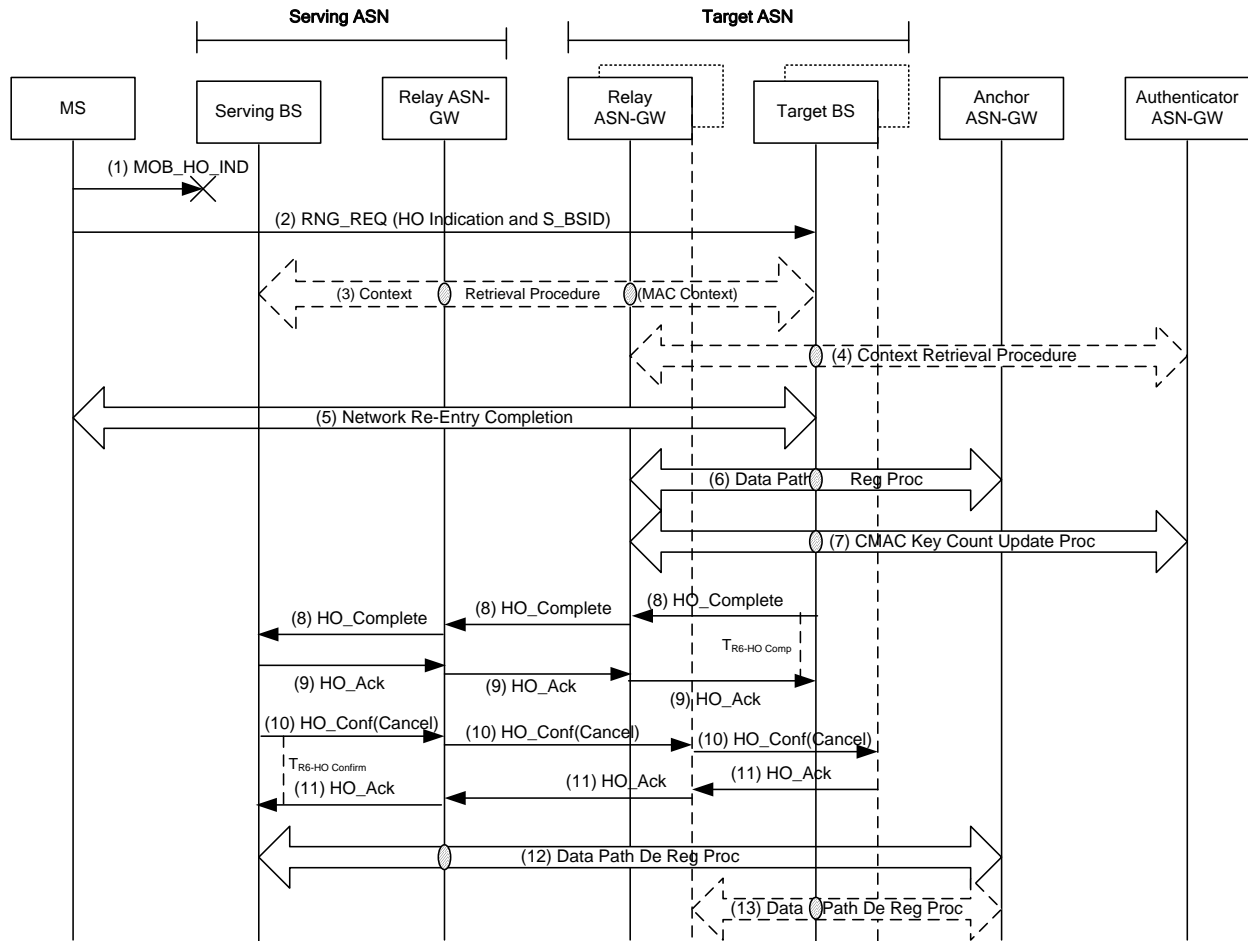
Upon receiving the *HO\_Complete* message, if the Serving BS has not deleted the data path previously and still has a data path with Anchor ASN-GW, the Serving BS SHALL initiate Data Path De-Registration procedure (see section 4.12) with the Anchor ASN-GW. Upon completing the Data Path Registration procedure with the Target BS, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure (see section 4.12) with the old Serving BS.

**STEP 14**

The Anchor ASN-GW SHALL de-register all the pre-registered data paths with the unselected Target BSs.

**4.7.2.2.2 Handover Action Scenario 2: HO\_Cnf not Received at Target BS**

The following call flow describes a successful inter-ASN Handover Action scenario where the *MOB\_HO-IND* sent by the MS to the Serving BS was lost over the air and not received by the Serving BS, and/or the *HO\_Cnf* message sent by the Serving BS to the Target BS was either delayed or not received. The MS completes network re-entry at one of the Target BSs selected by the Serving BS during the Handover Preparation phase.



**Figure 4-84 – Successful HO Action Phase, Scenario 2**

### STEP 1

The MOB\_HO-IND message is sent by the MS to the serving ASN-GW and lost over the air or not properly received by the Serving ASN-GW.

### STEP 2

The MS sends Ranging Request message with HO\_Indication and the serving BS ID information to one of the Target BSs that was indicated by the Serving BS during the Handover Preparation phase. If the Serving BS ID was not included, an initial network entry is required and initial network entry procedures SHALL be followed.

### STEP 3

The Target BS initiates a Context Request procedure (see section 4.12) with the Serving BS to retrieve the latest MAC context for the MS. This step is shown as optional in the Action phase.

### STEP 4

If an Authenticator ID TLV for the Authenticator ASN-GW was received in the HO\_Req or Context\_Req message but AK context was not obtained during the Handover Preparation phase, the Target BS requests AK context for the MS by initiating a Context Request procedure (see section 4.12) with the Authenticator ASN-GW.



**STEP 5**

After completing the retrieval of the MS context, the Target BS sends Ranging Response to the MS. The MS and Target BS complete the network Re-entry including the exchange of the required parameters (i.e., SBC-Req/Rsp).

**STEP 6**

The Target BS initiates a data path registration procedure (see section 4.12) with the Anchor ASN-GW. 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 BS initiates CMAC Key Count Update procedure (see section 4.12) and updates Authenticator ASNGW with the latest CMAC Key Count value which is received from MS.

**STEP 8**

Upon completion of network re-entry, the Target BS SHALL send a *HO\_Complete* message to the Serving BS to notify the completion of the handover. Relay ASN-GW relays the *HO\_Complete* message over R4/R6 to the Serving BS. Upon receipt of the *HO\_Complete* message, the Serving BS releases MS context and starts timer  $T_{R6\_HO\_Comp}$ .

**STEP 9**

The Serving BS sends a *HO\_Ack* message to the Target BS. Relay ASN-GW relays the *HO\_Ack* message over R4/R6. Upon receipt of the *HO\_Ack* message, the Target BS stops timer  $T_{R6\_HO\_Comp}$ .

**STEP 10**

The Serving BS may have already sent the *HO\_Cnf* message with the *HO\_Indication* type set to “Cancel” to some or all BSs. For all unselected Target BSs to which such message has not been sent yet, the Serving BS SHALL send such a message upon receipt of *HO\_Complete* message in order to clear the MS context at target ASNs/BSs. When Serving BS sends *HO\_Cnf* message it starts timer  $T_{R6\_HO\_Cnf}$ .

Relay ASN-GW relays the *HO\_Cnf* message over R6/R4.

**STEP 11**

The unselected Target BS sends an *HO\_Ack* message to the Serving BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Cnf}$ .

**STEP 12**

Upon receiving the *HO\_Complete* message, if the Serving ASN-GW has not deleted the data path previously and still has a data path with Anchor ASN-GW, the Serving BS SHALL initiate Data Path De-Registration procedure (see section 4.12.4 with the Anchor ASN-GW. Upon completing the Data Path Registration procedure with the Target BS, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure with the old Serving BS.

**STEP 13**

The Anchor ASN-GW SHALL de-register all the pre-registered data paths with the other (not selected) Target BSs.

**4.7.2.2.3 Handover Action Scenario 3: MOB\_HO-IND not received at Serving BS**

The following call flow describes a successful inter-ASN Handover Action scenario where the MOB\_HO-IND sent by the MS to the Serving BS was lost over the air and not received by the Serving BS. The MS completes network re-entry at one of the target BSs selected by the Serving BS during the Handover Action phase, or a target BS which wasn't notified of 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, or where the Serving BS doesn't receive MOB\_HO-IND because the message is lost in the air, and sends the *HO\_Cnf* messages to the entire set of the Target BSs (via Relay ASN-GW).

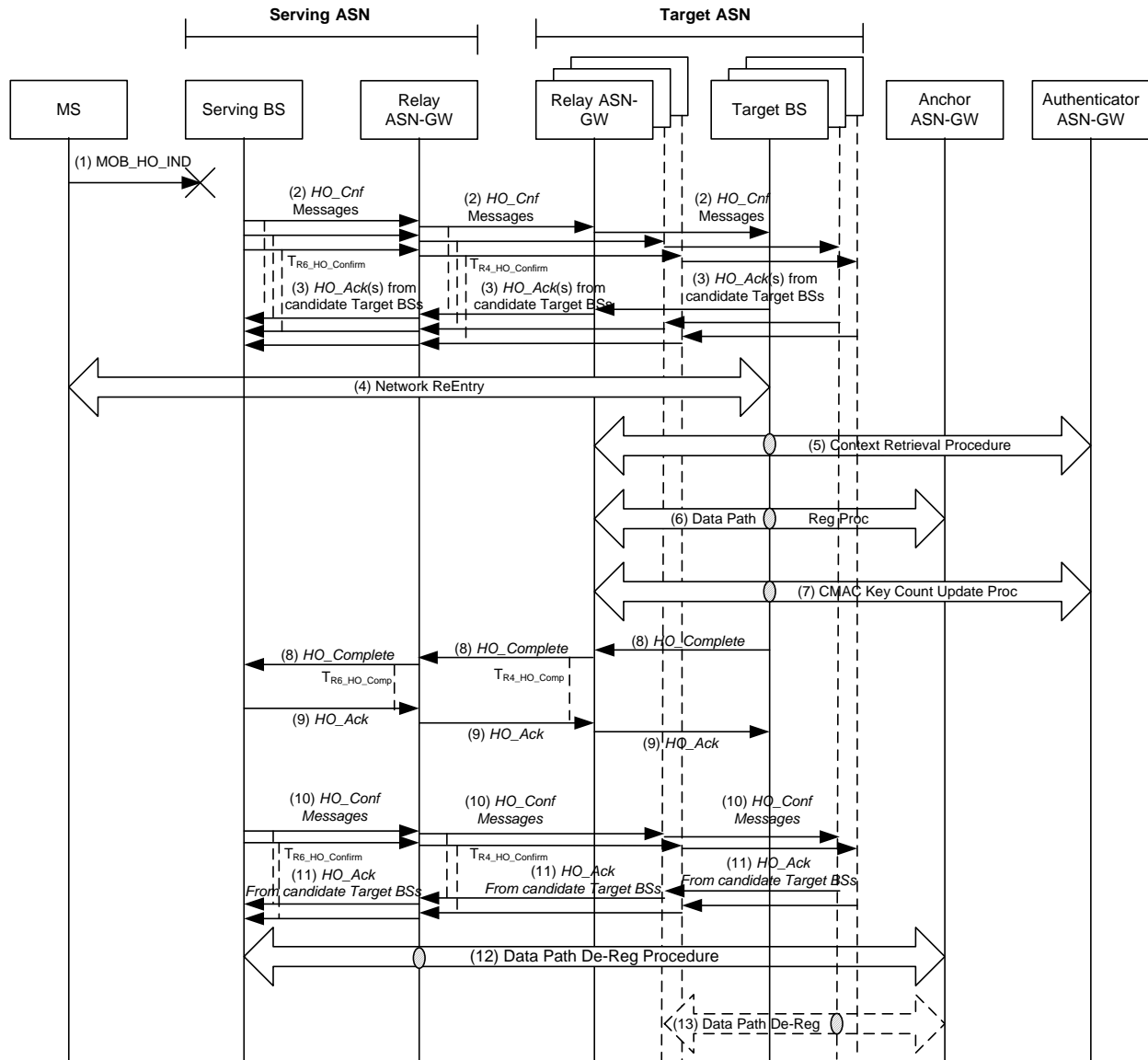


Figure 4-85 – Successful HO Action Phase, Scenario 3

### STEP 1

The MOB\_HO-IND sent by the MS to the Serving BS is lost over the air and not received by the Serving BS.

### STEP 2

Upon expiration of internal timer at the Serving BS, the Serving BS sends a *HO\_Cnf* message(s) with “Unconfirmed” type to the set of Target BS(s) controlling the candidate Target BS(s) which were indicated in the MOB\_BSHO-RSP or MOB\_BSHO-REQ and starts the  $T_{R6\_HO\_Conf}$  timer. The Serving BS also sends *HO\_Cnf* message to any candidate target BSs the MS may select to handover to which weren’t previously notified of a potential handover from the MS during the handover preparation. The *HO\_Cnf* message contains the HO\_Indication Type set to “Unconfirmed”, Authenticator GW ID or AK context, Anchor ASN-GW ID, and latest MAC context information.

Relay ASN-GW relays the *HO\_Cnf* message over R6/R4.

**STEP 3**

Each Target BS sends *HO\_Ack* message to the serving BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops the corresponding  $T_{R6\_HO\_Conf}$  timer.

**STEP 4**

The MS completes network re-entry at one of the target BSs selected by the Serving BS during the Handover Action phase, or at a target BS notified of an impending handover from the MS after the serving BS detects the loss of communication with the MS due to loss of the MOB\_HO-IND message.

**STEP 5**

If the Authenticator ID was included in the *HO\_Req* or *HO\_Cnf* message and AK context was not obtained during the Handover Preparation phase, the Target BS requests AK context for the MS by initiating a Context Request procedure (see section 4.12) with the Authenticator ASN-GW.

**STEP 6**

If the Anchor ASN GW ID TLV was included in the *HO\_Req* or *HO\_Cnf* message received during the Handover Preparation phase and data path pre-registration did not occur, the Target BS initiates a Data Path Registration procedure (see section 4.12) with the Anchor ASN-GW. This step can be executed any time after receiving *HO\_Cnf* message.

**STEP 7**

Target BS initiates CMAC Key Count Update procedure (see section 4.12) and updates Authenticator ASN-GW with the latest CMAC Key Count value which is received from MS.

**STEP 8**

The Target BS SHALL send an *HO\_Complete* message to the Serving BS to expedite release of MS context information. Relay ASN-GW relays the *HO\_Complete* message over R6/R4. Upon receipt of the *HO\_Complete* message, the Serving BS releases the MS context and stops the Resource Retain Timer and starts timer  $T_{R6\_HO\_Comp}$ .

**STEP 9**

The Serving BS sends a *HO\_Ack* message to the Target BS via Relay ASN-GW. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Comp}$ .

**STEP 10**

The Serving BS may have already sent the *HO\_Cnf* message with the HO\_Indication type set to “Cancel” to some or all Target BSs. For all unselected Target BSs to which such message has not been sent yet, the Serving BS SHALL send such a message upon receipt of *HO\_Complete* message in order to clear the MS context at target BSs. When Serving BS sends *HO\_Cnf* message it starts timer  $T_{R6\_HO\_Conf}$ .

Relay ASN-GW relays the *HO\_Cnf* message over R6/R4.

**STEP 11**

The unselected Target BS sends a *HO\_Ack* message to the Serving BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Conf}$ .

**STEP 12**

Upon receiving the *HO\_Complete* message, if the Serving BS has not deleted the data path previously and still has a data path with Anchor ASN-GW, the Serving BS SHALL initiate Data Path De-Registration procedure with the Anchor ASN-GW. Upon completing the Data Path Registration procedure with the Target BS, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure with the old Serving BS.

**STEP 13**

The Anchor ASN-GW SHALL de-register all the pre-registered data paths with the other (not selected) Target BSs.

**4.7.2.2.4 Handover Action Scenario 4: Anchor ASN-GW and Anchor Authenticator Collocated with Serving ASN-GW – Serving ASN-GW Initiates Path Registration**

The following call flow describes a successful inter-ASN handover action scenario where the Anchor ASN-GW is collocated with the Serving ASN-GW and the Authenticator ASN-GW and the Serving/Anchor ASN-GW initiates Data Path Registration procedure with the Target BS during the Handover Action phase. The Target BS receives the *HO\_Cnf* message from the Serving BS via the Relay ASN-GW.

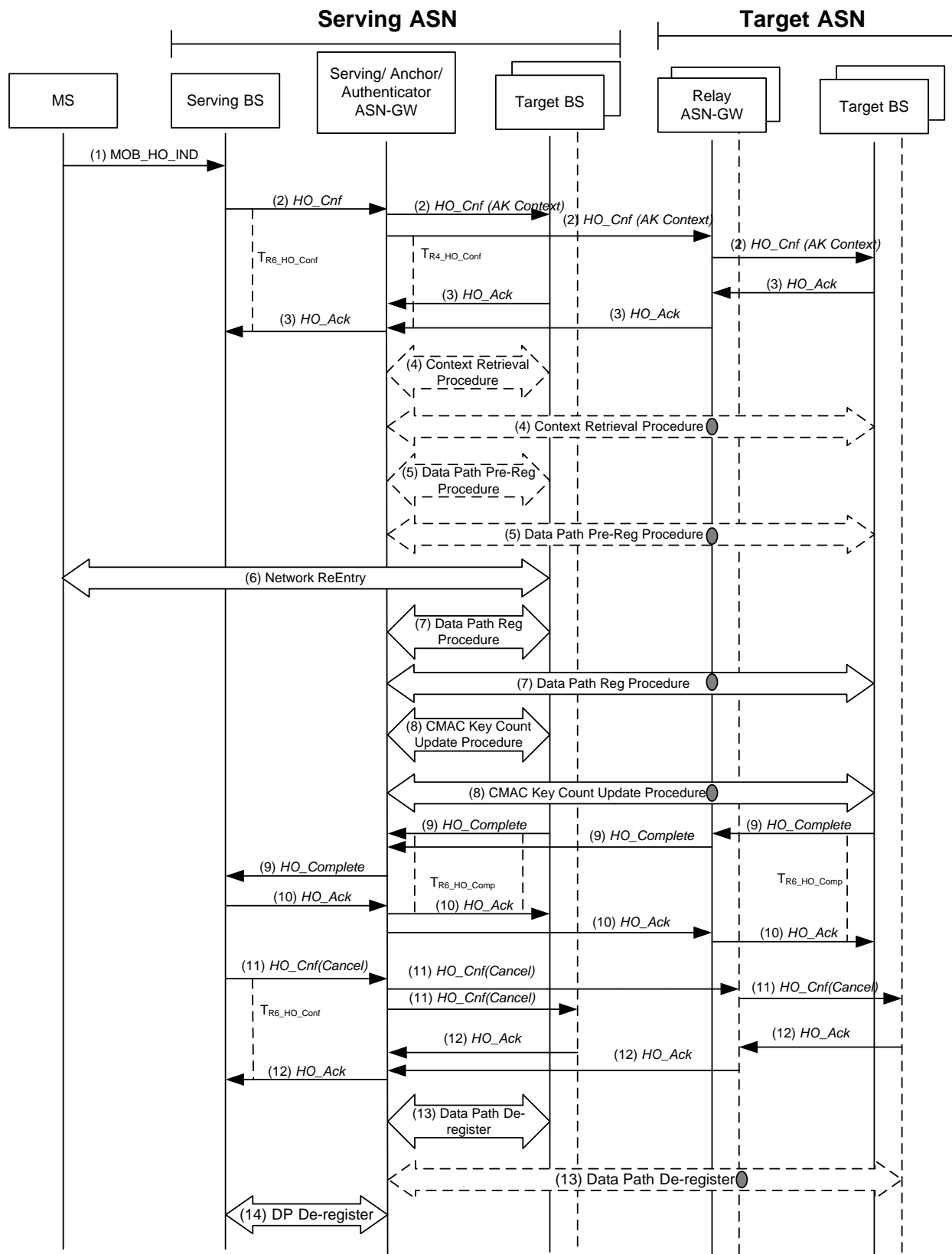


Figure 4-86 – Successful HO Action Phase, Scenario 4

**STEP 1**

The MS sends a MOB\_HO-IND to the Serving BS to notify a handover to one of the Target BSs candidates selected by the Serving BS during the Handover Preparation phase.

**STEP 2**

Upon reception of the MOB\_HO-IND the Serving BS sends an *HO\_Cnf* message and starts timer  $T_{R6\_HO\_Conf}$ . Serving BS MAY also send *HO\_Cnf* message with the value of the HO\_Indication type set to “Cancel” to all unselected Target BS(s) and clear the MS context.

The Serving BS sends an *HO\_Cnf* message to the Target BS and starts timer  $T_{R4\_HO\_Conf}$ . Serving BS MAY also send an *HO\_Cnf* message with the value of the HO\_Indication type set to “Cancel” to all unselected Target BS(s) and clear the MS context.

Relay ASN-GW relays the *HO\_Cnf* message over R6/R4.

In case where the Serving ASN-GW is collocated with the Authenticator ASN-GW, upon reception of the *HO\_Cnf* from the Serving BS, the Serving ASN-GW MAY send the piggybacked AK Context with *HO\_Cnf* message.

In case where the Serving ASN-GW is collocated with the Anchor ASN-GW, upon reception of the *HO\_Cnf* from the Serving BS, the Anchor ASN-GW MAY send the piggybacked Data Path Info TLV with *HO\_Cnf* message.

**STEP 3**

The Target BS sends an *HO\_Ack* message to the Serving BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Conf}$ .

**STEP 4**

If the Serving BS doesn't support the piggybacked AK Context, the Serving BS may initiate a context retrieval procedure with the Authenticator ASN-GW.

**STEP 5**

The Serving BS may initiate a Data Path Pre-Registration procedure (see section 4.12) with the Target BS if Data Path Pre-Registration did not occur. If the Target BS doesn't support Anchor ASN-GW initiated Data Path Pre-Registration procedure, it may initiate the procedure on its own.

**STEP 6**

The MS initiates network re-entry with the Target BS.

**STEP 7**

If not already established, the Target BS initiates a Data Path Registration procedure (see section 4.12) with the Anchor ASN-GW. This step can be executed any time after receiving *HO\_Cnf* message.

**STEP 8**

Upon successful completion of network re-entry, the Target BS initiates CMAC Key Count Update procedure (see section 4.12) and updates the Authenticator ASN-GW with the latest CMAC Key Count value which is received from MS.

**STEP 9**

Upon completion of network entry, the target BS SHALL send a *HO\_Complete* message to the serving BS to acknowledge the completion of the handover. Relay ASN-GW relays the *HO\_Complete* message over R6/R4. Upon receipt of the *HO\_Complete* message, the Serving BS SHALL release the MS context and starts timer  $T_{R6\_HO\_Comp}$ .

**STEP 10**

The Serving BS sends a *HO\_Ack* message to the Target BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Comp}$ .

**STEP 11**

Upon receiving the *HO\_Complete* message, if Serving BS did not send *HO\_Cnf* message with the value of the *HO\_Indication* type set to “Cancel” to all unselected Target BS(s) in STEP 2, it SHALL send an *HO\_Cnf* message with the value of the *HO\_Indication* type set to “Cancel” to all unselected Target BS(s) to clear the MS context and starts timer  $T_{R6\_HO\_Cnf}$ .

Relay ASN-GW relays the *HO\_Complete* message over R6/R4.

**STEP 12**

The unselected Target BS sends a *HO\_Ack* message to the Serving BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R4\_HO\_Cnf}$ .

**STEP 13**

If pre established during HO preparation stage, the Anchor ASN-GW SHALL de-register all the pre-registered data paths with the other not selected Target BSs candidates.

**STEP 14**

The Serving/Anchor ASN-GW deregisters the data path with (old) serving BS.

**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 BS(s) 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 message(s) 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. The trigger for sending the *HO\_Cnf(cancel)* message is receipt of the *MOB\_HO\_IND* message with the indication to cancel the handover procedure; anytime after receipt of a *MOB\_HO\_IND* message with indication of a handover to the target BS selected as part of preparation stage, or the *HO\_Complete* message received by the serving BS when the MS completes the network re-entry at the target BS.

Note: The term “Unselected Target BS” in the following figures for various HO Cancellation scenarios refers to the Target BS that had been selected as the potential target BS that the MS may handover to, and which includes at least one Target BS that has not been selected for HO.

#### 4.7.2.3.1 HO Cancellation Scenario 1: Serving and Anchor ASN-GW are Collocated and “Unselected Target BS” Receives HO\_Cnf from Serving BS

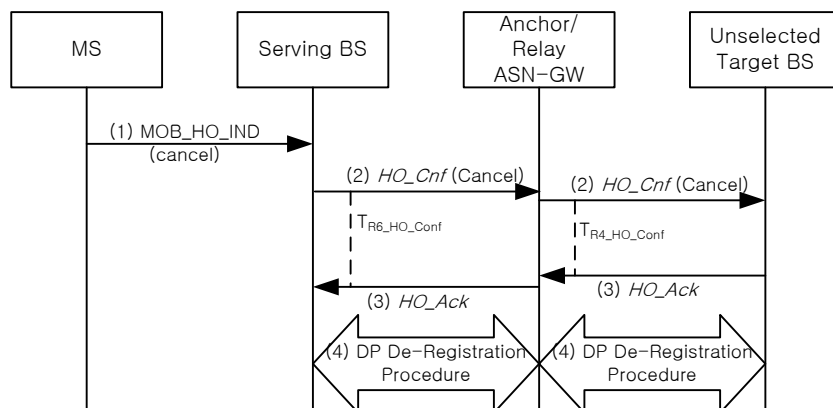


Figure 4-87 – R4 HO Cancellation, Scenario 1

##### STEP 1

The MS sends MOB\_HO\_IND to the Serving BS. In the MOB\_HO\_IND, the MS indicates, that it decided to cancel the handover procedure, 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 *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  $T_{R6\_HO\_Conf}$ . If the timer expires, the Serving BS may re-send the *HO\_Cnf*. After a pre-defined number of retransmissions, the Serving BS stops resending the *HO\_Cnf*. The Target BS SHALL perform the local clean up if *HO\_Cnf* is never received from the Serving BS. Relay ASN-GW relays the *HO\_Ack* message over R6/R4 and starts  $T_{R4\_HO\_Conf}$ .

##### STEP 3

If the Target BS receives the *HO\_Cnf* with HO\_Indication type set to “Cancel”, the Target BS sends *HO\_Ack* to the Serving BS and releases the pre-allocated system resources, which are to support the MS handover. The Target BS may also initiate the Data Path De-Registration Procedure (section 4.12.4) towards the Anchor ASN-GW if a DP had been pre-established.

##### STEP 4

Upon expiry of the MS Context Retain Timer, the Serving BS may start the Data Path De-Registration Procedure (section 4.12.4) to the Anchor ASN-GW. Also the Anchor ASN-GW may start Data Path De-Registration Procedure (section 4.12.4) with the Unselected Target BS if Path Pre-Registration or Path Registration has been received by the Target BS during the HO Preparation phase. If the MS is no longer attached to the Serving BS, the Serving BS SHALL release all the allocated system resource for the MS.



#### 4.7.2.3.2 HO Cancellation Scenario 2: Serving and Anchor ASN-GW are not Collocated and “Unselected Target BS” receives HO\_Cnf from Serving BS

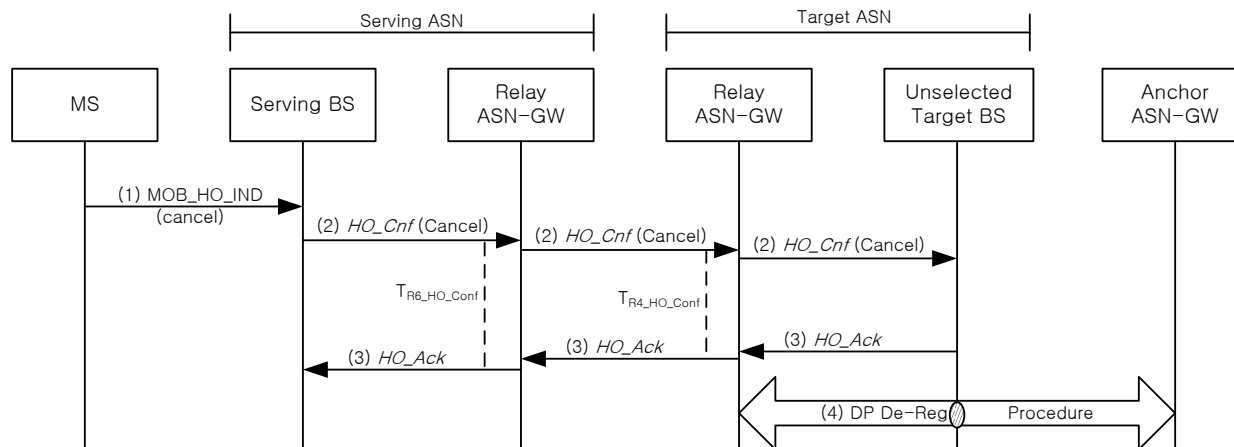


Figure 4-88 – R4 HO Cancellation, Scenario 2

##### STEP 1

The MS sends MOB\_HO-IND to the Serving BS. In the MOB\_HO-IND, the MS indicates, that it decided 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 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 awaits HO\_Ack by starting the  $T_{R6\_HO\_Cnf}$ . Relay ASN-GW relays the message over R6/R4 and starts timer  $T_{R4\_HO\_Cnf}$ . If the timer expires, the Serving BS may re-send the HO\_Cnf. After a pre-defined number of retransmissions, the Serving BS stops resending the HO\_Cnf. The Target BS SHALL perform the local clean up if HO\_Cnf is never received from the Serving BS.

##### STEP 3

Target BS receives the HO\_Cnf with HO\_Indication type set to “Cancel”. Target BS sends HO\_Ack to the Serving BS and may release the pre-allocated system resources, which are to support the MS handover. Relay ASN-GW relays the message over R6/R4.

##### STEP 4

The Target BS may start the Data Path De-Registration Procedure (section 4.12.4) to the Anchor ASN-GW if data path has already been established between the Target BS and the Anchor ASN-GW. If the MS is no longer attached to the Serving BS, the Serving BS SHALL release all the allocated system resource for the MS.

### 4.7.2.3.3 HO Cancellation Scenario 3: A subset of the Target BS(s) does not Receive HO\_Cnf(Cancel).

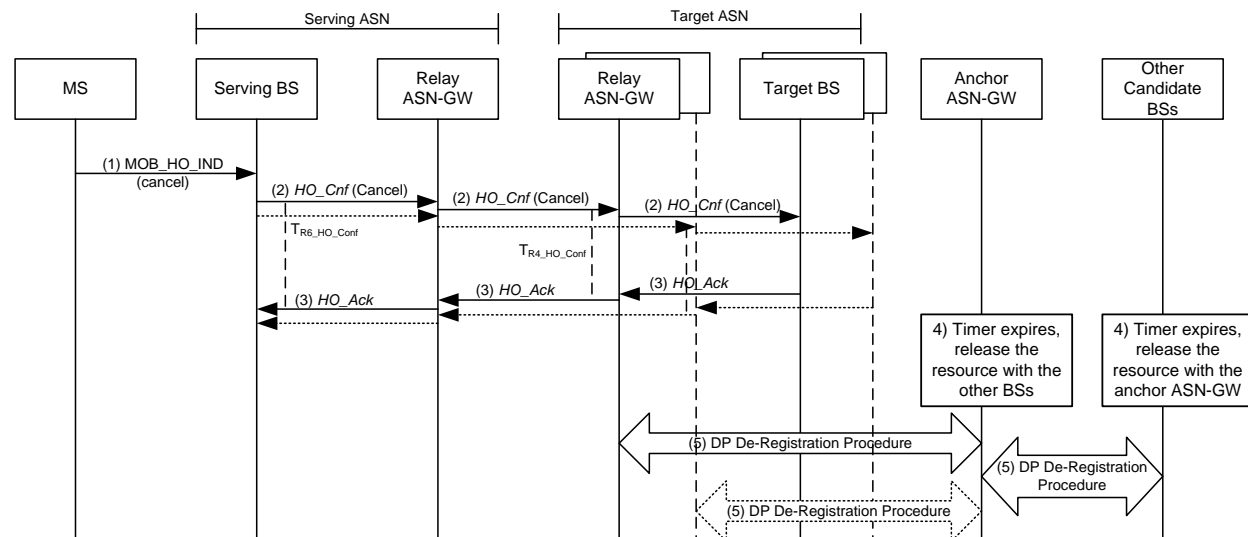


Figure 4-89 – HO Cancellation, Scenario 3

#### STEP 1

The MS sends MOB\_HO-IND to the Serving BS. In the MOB\_HO-IND, the MS indicates, that it decided 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 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 including CMAC context that are prepared for the MS to handover. After sending the message, the Serving BS awaits HO\_Ack by starting the  $T_{R6\_HO\_Cnf}$ . Relay ASN-GW relays the message over R6/R4 and starts timer  $T_{R4\_HO\_Cnf}$ . If the timer expires, the Serving BS may re-send the HO\_Cnf. After a pre-defined number of retransmissions, the Serving BS stops resending the HO\_Cnf. The Target BS SHALL perform the local clean up if HO\_Cnf is never received from the Serving BS.

#### STEP 3

The Target BS(s) sends a HO\_Ack to the serving BS and releases the MS resources. Relay ASN-GW relays the message over R6/R4. Upon receipt of the HO-Ack message, the Serving BS stops timer  $T_{R6\_HO\_Cnf}$ .

#### STEP 4

If one of the Target BSs does not receive the HO\_Cnf, upon a timer expiry the Target BS releases the pre-allocated system resources, and if obtained the MS context, which are to support the MS handover.

#### STEP 5

After receiving HO\_Cnf (Cancel) or after the timer associated with the pre-registered DP expires, the Target BS(s) may start the Path\_Deregistration Procedure (4.12.4), through the relay ASN-GW, to the Anchor ASN-GW if data path has already been established between the Target BS(s) and the Anchor ASN-GW. If the MS is no longer attached to the Serving BS, the Serving BS SHALL release all the allocated system resource for the MS.

#### 4.7.2.3.4 HO Cancellation Scenario 4: Serving BS receives HO\_Complete

In this scenario the MS successfully completes the network re-entry procedure at a target BS. Note that the target BS where the MS re-entered may be different from the BS indicated in the MOB\_HO\_IND message at the start of the HO action phase.

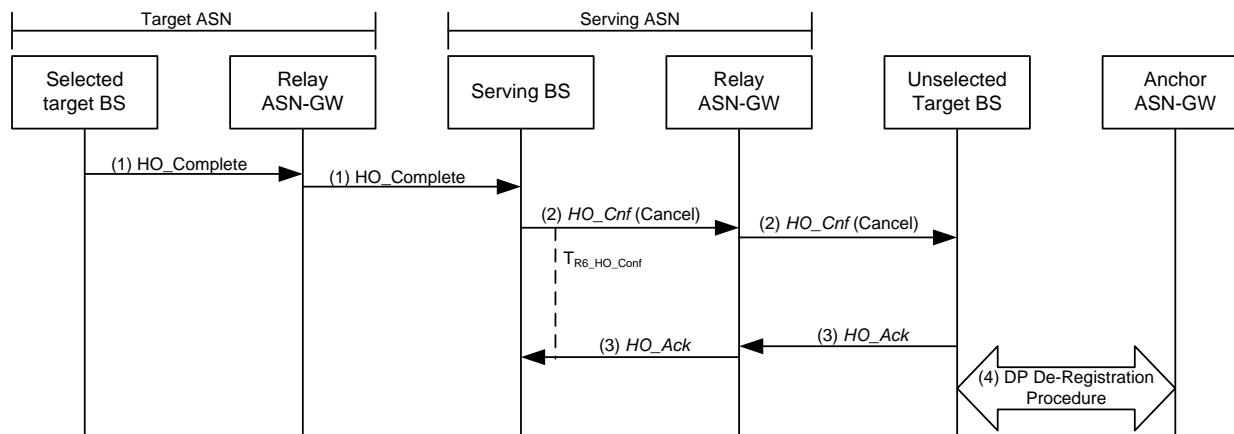


Figure 4-90 – HO Cancellation, Scenario 4

#### STEP 1

The BS where the MS completed network re-entry sends HO\_Complete message to the serving BS. Relay ASN-GW relays the message over R6/R4.

#### STEP 2

Receiving the HO\_Complete message causes the Serving BS, (if it has not already sent a prior HO\_Cnf message with the value of the HO\_Indication type set to “Cancel” once to all unselected Target BS(s)) to send HO\_Cnf message with the value of the HO\_Indication type set to “Cancel” to inform the previously selected potential Target BS(s) to de-allocate the reserved system resources that are prepared for the MS to handover. Relay ASN-GW relays the message over R6/R4 and starts timer  $T_{R4\_HO\_Cnf}$ . After sending the message, the Serving BS awaits for the HO\_Ack message by starting the  $T_{R6\_HO\_Cnf}$ . If the timer expires, the Serving BS may re-send the HO\_Cnf. After a pre-defined number of retransmissions, the Serving BS stops resending the HO\_Cnf. The Target BS SHALL perform the local clean up if HO\_Cnf is never received from the Serving BS.

#### STEP 3

Each unselected Target BS sends HO\_Ack to the Serving BS and releases the pre-allocated system resources, which are to support the MS handover. Relay ASN-GW relays the message over R6/R4. Upon the resource retain timer expiry, if the MS is no longer attached to the Serving BS, the Serving BS SHALL release all the allocated system resource for the MS.

#### STEP 4

If the Target BS still have DP pre-established with the Anchor ASN-GW, the Target BS may also initiate the data Path de-registration procedure (section 4.12.4).

Note:

If the serving BS receives neither the MOB\_HO\_IND message nor the HO\_Complete message, upon the expiration of the internal timer the serving BS SHOULD send a HO\_Confirm(cancel) message to all the candidate target BSs.

#### 4.7.2.4 MS Handover Rejection

The following call flow describes the scenario when the MS rejects target BSs offered to it by the Serving BS for handover.

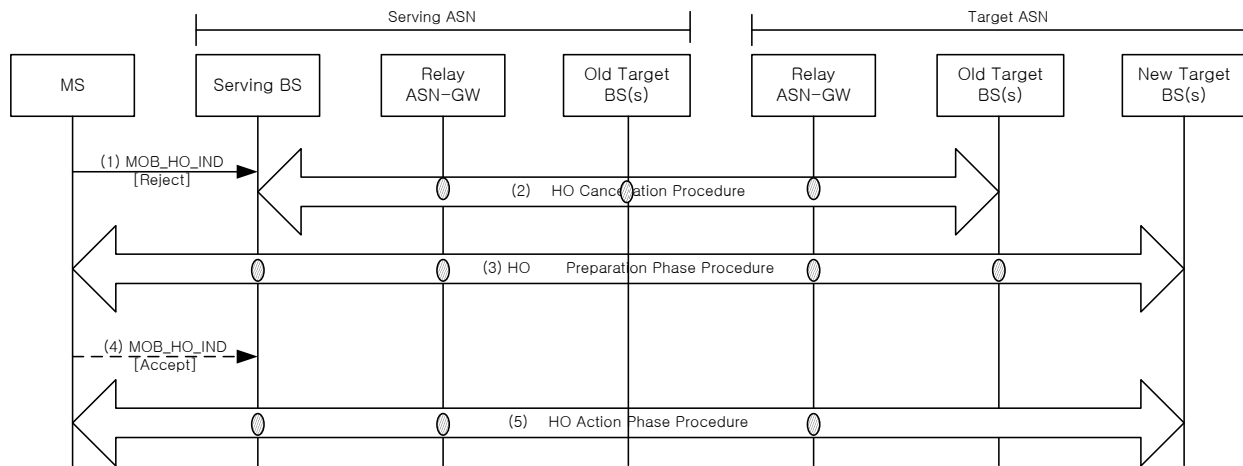


Figure 4-91 – MS Handover Rejection

##### STEP 1

The MS sends a MOB\_HO-IND containing HO\_IND\_Type TLV set to 0b10 indicating rejection of the target BS(s) offered by the serving BS for handover in the MOB\_BSHO-RSP (MS initiated handover) or MOB\_BSHO-REQ (network initiated handover) message.

##### STEP 2

The serving BS initiates the handover cancellation procedures described in section 4.7.2.3 with the Target BS(s) controlling the target BS(s) which were rejected for handover by the MS.

The following steps only occur if the Serving BS is able to offer an alternate target BS(s) to the MS.

##### STEP 3

The Serving BS starts network initiated HO described in 7.4.2.1.6 and initiates the handover preparation procedures with a Target BS(s) to be offered to the MS for handover.

##### STEP 4

The MS indicates acceptance of a new target BS offered by the Serving BS to the MS for handover in the MOB\_BSHO-RSP (MS initiated) or MOB\_BSHO-REQ (network initiated) message, by sending a MOB\_HO-IND message with HO\_IND\_Type TLV set to 0b00.

##### STEP 5

The Serving BS completes the handover action procedures described in section 4.7.2.2 and the MS completes successful handover to the new target BS.

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 Serving BS decides to offer a new target BS for handover to the MS, steps 3-5 are repeated.

#### 4.7.2.5 HO Action Phase Timers and Timing Considerations

This section identifies the timer entities participating in the HO Action Phase. The following timers are defined over R6:

- $T_{R6\_Path\_Reg\_Req}$ : 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.
- $T_{R6\_Path\_Reg\_Rsp}$ : is started by the Anchor 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 Anchor ASN-GW after completion of the Data Path Registration procedure for an MS, upon sending the *R6 Path\_Dereg\_Req* message, and is stopped upon receiving a corresponding *R6 Path\_Dereg\_Rsp* message.
- $T_{R6\_CMAC\_Key\_Count\_Upd}$ : is started by a Target (now new Serving) BS after MS completes network re-entry, upon sending the *R6 CMAC\_Key\_Count\_Update* message to the Authenticator ASN, and is stopped upon receiving a corresponding *R6 CMAC\_Key\_Count\_Update\_Ack* message from the Authenticator ASN.
- $T_{R6\_HO\_Conf}$ : is started by the Serving BS when sending a *R6 HO\_Cnf* message to a Target BS, and is stopped upon receiving a *R6 HO\_Ack* message from the corresponding Target BS.
- $T_{R6\_HO\_Comp}$ : is started by the Target (now new Serving) BS after MS completes network re-entry, upon sending the *R6 HO\_Complete* message to the Serving BS, and is stopped upon receiving a corresponding *R6 HO\_Ack* message from the Serving BS.

This section identifies the timer entities participating in the HO Action Phase. The following timers are defined over R4:

- $T_{R4\_Path\_Reg\_Req}$ : is started by the Target ASN to initiate establishment or provide confirmation of the data paths for an MS, upon sending the *R4 Path\_Reg\_Req* message, and is stopped upon receiving a corresponding *R4 Path\_Reg\_Rsp* message.
- $T_{R4\_Path\_Reg\_Rsp}$ : is started by the Anchor ASN upon sending the *R4 Path\_Reg\_Rsp* message if no data path has been pre-established for the MS, and is stopped upon receiving a corresponding *R4 Path\_Reg\_Ack* message.
- $T_{R4\_DP\_De\_Reg\_Req}$ : is started by the Anchor ASN after completion of the Data Path Registration procedure for an MS, upon sending the *R4 Path\_Dereg\_Req* message, and is stopped upon receiving a corresponding *R4 Path\_Dereg\_Rsp* message.
- $T_{R4\_CMAC\_Key\_Count\_Upd}$ : is started by a Target (now new Serving) ASN after MS completes network re-entry, upon sending the *R4 CMAC\_Key\_Count\_Update* message to the Authenticator ASN, and is stopped upon receiving a corresponding *R4 CMAC\_Key\_Count\_Update\_Ack* message from the Authenticator ASN.
- $T_{R4\_HO\_Conf}$ : each such timer is started by the serving ASN when sending the *R4 HO\_Cnf* message to each of the candidate Target ASNs. Each timer is stopped upon receiving a *R4 HO\_Ack* message from the corresponding Target ASN.
- $T_{R4\_HO\_Comp}$ : is started by the Target (now new Serving) ASN after MS completes network re-entry, upon sending the *R4 HO\_Complete* message to the Serving ASN, and is stopped upon receiving a corresponding *R4 HO\_Ack* message from the Serving ASN.

Table 4-80 shows the default value of timers and also indicates the range of the recommended duration of these timers. Note that these values are provisioned in the current Release.

**Table 4-80 – HO Action Phase R4 and R6 Timer Values**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R6\_Path\_Reg\_Req}$	TBD		TBD
$T_{R6\_Path\_Reg\_Rsp}$	TBD		TBD

T <sub>R6_Path_De-Reg_Req</sub>	TBD		TBD
T <sub>R6_Path_De-Reg_Req</sub>	TBD		TBD
T <sub>R6_CMACE_Key_Count_Upd</sub>	TBD		TBD
T <sub>R6_HO_Conf</sub>	TBD		TBD
T <sub>R6_HO_Comp</sub>	TBD		TBD
T <sub>R4_Path_Reg_Req</sub>	TBD		TBD
T <sub>R4_Path_Reg_Rsp</sub>	TBD		TBD
T <sub>R4_Path_De-Reg_Req</sub>	TBD		TBD
T <sub>R4_Path_De-Reg_Rsp</sub>	TBD		TBD
T <sub>R4_CMACE_Key_Count_Upd</sub>	TBD		TBD
T <sub>R4_HO_Conf</sub>	TBD		TBD
T <sub>R4_HO_Comp</sub>	TBD		TBD

#### 4.7.2.6 HO Action Phase Error Conditions

This section describes error conditions associated with the HO Action Phase.

##### 4.7.2.6.1 Timer Expiry

Table 4-81 shows details on the corresponding actions associated with timer expiry. Upon each timer expiry, if the maximum retries has not exceeded, the related message is retransmitted and the timer is restarted. Otherwise, the corresponding action(s) should be performed as indicated in Table 4-80.

**Table 4-81 – Actions after MAX Re-transmit Retries**

Timer	Entity where Timer Started	Action(s)
T <sub>R6_Path_Reg_Req</sub>	Target BS	BS shall force MS to perform initial network entry.
T <sub>R6_Path_Reg_Rsp</sub>	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 <sub>R6_Path_De-Reg_Req</sub>	Anchor ASN-GW	No action required.
T <sub>R6_Path_De-Reg_Rsp</sub>	BS	
T <sub>R6_CMACE_Key_Count_Upd</sub>	Target (new Serving) BS	BS shall force MS to perform initial network entry.
T <sub>R6_HO_Cnf</sub>	(old) Serving BS	No action required.
T <sub>R6_HO_Comp</sub>	Target BS	No action required.
T <sub>R4_Path_Reg_Req</sub>	Target ASN-GW	ASN-GW SHALL force MS to perform initial network entry.
T <sub>R4_Path_Reg_Rsp</sub>	Anchor ASN-GW	ASN-GW SHALL defer sending the downlink packets until it receives any packets for MS from Target(new Serving) ASN-GW. ASN-GW SHALL reset data paths for MS if no packets are received until a pre-specified system timer expires.

T <sub>R4_Path_De-Reg_Req</sub>	Anchor ASN-GW	No action required.
T <sub>R4_Path_De-Reg_Rsp</sub>		
T <sub>R4_CMAC_Key_Count_Upd</sub>	Target (new Serving) ASN-GW	ASN-GW SHALL force MS to perform initial network entry.
T <sub>R4 HO Comp</sub>	Target ASN-GW	No action required.

#### 4.7.2.6.2 Path\_Reg\_Rsp Error

Upon receipt of the *Path\_Reg\_Req* message, if the Anchor ASN-GW is unable to support the requested establishment of the data path(s), then it SHALL send a *Path\_Reg\_Rsp* message with suitable error code.

Upon receipt of the *Path\_Reg\_Rsp* message with suitable error code, the Target (new serving) BS/ASN-GW SHALL stop T<sub>R6-DP\_Reg-Req</sub>/T<sub>R4-DP\_Reg-Req</sub> (if running). The Target BS/ASN-GW MAY re-send the *Path\_Reg\_Req* message. If the Target BS/ASN-GW does not resend the *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.

#### 4.7.2.6.3 HO\_Cnf Error

If the timer T<sub>R6\_HO\_Cnf</sub> expires, the Serving BS may re-send the *HO\_Cnf*. After a pre-defined number of retransmissions, the Serving BS stops resending the *HO\_Cnf*. The Target BS SHALL perform the local clean up if *HO\_Cnf* is never received from the Serving BS.

### 4.7.3 Uncontrolled (Unpredictive) HO with Context Retrieval

An Uncontrolled (Unpredictive) handover occurs when an MS starts ranging at a Target BS that wasn't previously notified of an impending handover from an MS and didn't participate in the Handover Preparation Phase. This may occur due to suboptimal radio planning conditions or MS implementation (handover notification to the network by the BS is optional).

If an MS starts ranging with a BS that doesn't have MS Context information including Authenticator ASN-GW and Anchor ASN-GW identifiers, the RNG-REQ message from the MS cannot be authenticated. In a worst case scenario an initial Network Re-Entry will be required which results in large delays, because some authentication methods may take seconds to complete, especially if the Home AAA Server is located far away and the communication is slow.

However if the MS includes the Serving BS ID TLV in the RNG-REQ message, the handover can still be completed and the period of traffic unavailability can be greatly reduced. When an MS re-enters at a Target BS and supplies its Serving BS ID in the RNG-REQ message, the Target BS may retrieve the relevant MS Context from the Serving BS including the Authenticator ID and Anchor ASN-GW ID, and optionally AK Context information. Thus it becomes possible to retrieve the Authenticator Context for the MS to authenticate the RNG-REQ and perform data path registration with the Anchor DP ASN-GW. This call flow scenario is described in Figure 4-92.

If the Anchor ASN GW ID is not included in the *Context\_Rpt*, the Serving ASN-GW hosts the Anchor data path function for the MS and data path registration occurs with the Serving ASN-GW. The content of the messages are described in sections 4.7.5.1 and 4.7.5.2. If the serving ASN-GW is co-located with the Authenticator ASN-GW, the serving ASN-GW MAY provide the piggybacked AK context information to the target BS in the *Context\_Rpt*.

Network Re-Entry might be completed immediately after receiving the MS Context or after data path establishment (the latter case is shown in the call flows)<sup>10</sup>. The moment of Network Re-Entry completion does not affect interoperability and is left as a vendor implementation option.

<sup>10</sup> 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.

### 4.7.3.1 Successful Uncontrolled Handover

The following call flow provides an example of a successful uncontrolled handover scenario. A MS begins ranging at Target BS that wasn't contacted by the Serving BS to participate in the Handover Preparation phase. Therefore the Target BS was unaware of an impending hand-in from the MS. The MS includes the Serving BS ID in the RNG-REQ message. The Target BS retrieves the MS context and authenticator information and successfully completes the handover.

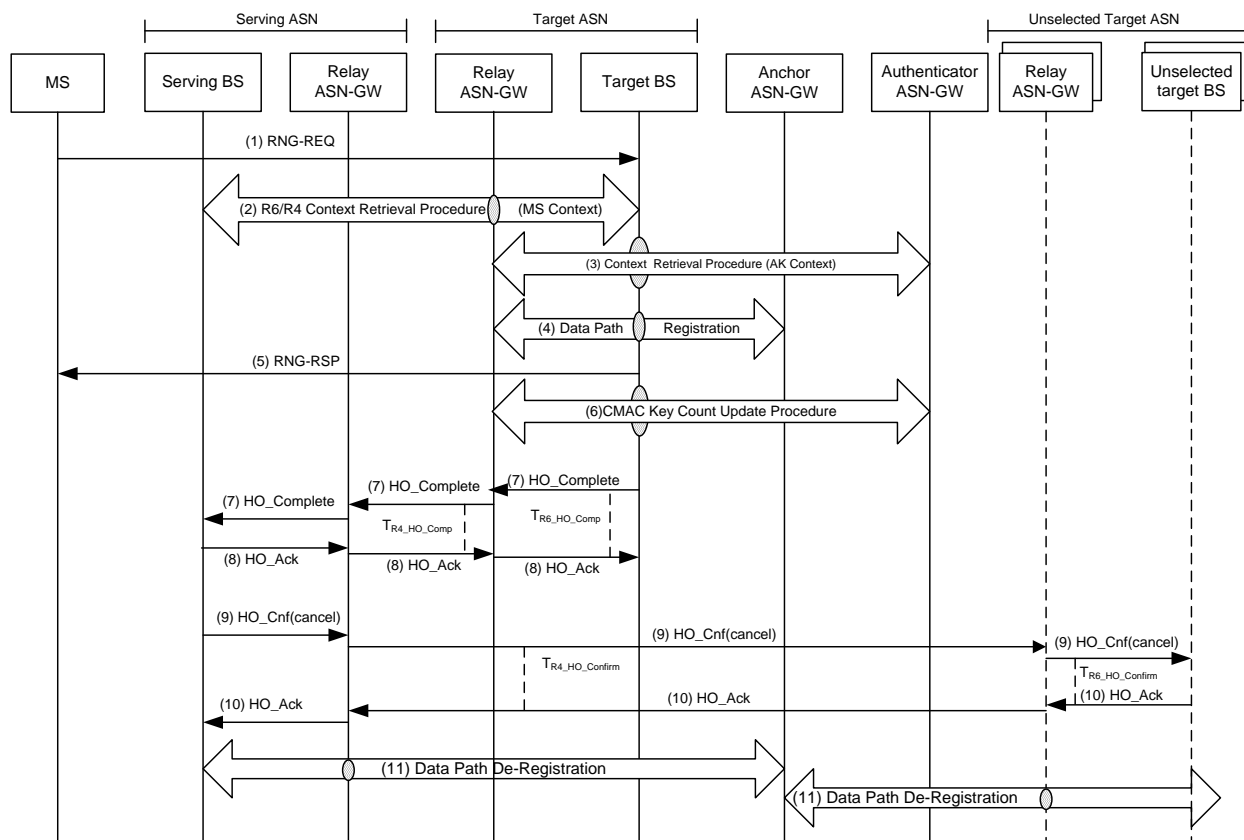


Figure 4-92 – Uncontrolled (Unpredictive) HO

#### STEP 1

An MS performs an uncontrolled handover by sending a RNG-REQ message to perform contention based ranging at a Target BS that didn't receive prior notification of an impending handover from the MS and therefore didn't participate in the Handover Action/Preparation phase. The MS includes the Serving BSID TLV in the RNG-REQ message.

#### STEP 2

The Target BS initiates a Context Request procedure with the Serving BS to retrieve context information for the MS. See section 4.12 for this procedure. The Serving BS responds by sending the context information which includes the Anchor Authenticator ID and Anchor ASN-GW ID. Optionally, if the Target BS requests also the delivery of AK Context information by setting appropriate bits of Context Purpose Indicator TLV, and if the Serving ASN-GW is collocated with the Authenticator ASN-GW and supports the piggybacking AK Context feature, the Serving ASN-GW may include the piggybacked AK Context in the response message sent to the Target BS. If the Authenticator ASN ID and/or Anchor ASN ID was not sent, the Serving ASN-GW hosts the respective functions. If the MS mobility access classifier is fixed or nomadic and the BS supports mobility restriction for stationary access, if the



target BS does not belong to the Reattachment zone, then the target BS directs the MS to start an initial network entry.

### STEP 3

The Target BS requests AK context for the MS by initiating a Context Request procedure with the Authenticator ASN-GW. See section 4.12 for this procedure. If no authenticator ID was received (Serving ASN-GW is co-located with the Authenticator ASN-GW), the Target BS initiates a Context Request procedure with the Authenticator ASN-GW.

If the MS' mobility access classifier is fixed or nomadic, the MS' Authenticator will reject AK context requests from the unauthorized Target BSs based on Authenticator's knowledge of MS Reattachment Zone list. To reject the AK context request from the Target BS, the MS' Authenticator responds with Context-Rpt message that includes appropriate Failure Indication value and excludes MS' AK context.

In this case the Target BS will direct the MS to start an initial network entry.

### STEP 4

The Target BS initiates data path registration for the MS with the Anchor ASN-GW. See section 4.12 for this procedure. If the Anchor ASN-GW ID was not sent to it as part of the MS context from the Serving BS, the Serving ASN-GW hosts the Anchor data path function and the Target BS initiates Data Path Registration procedure (see section 4.12) for the MS with the Anchor ASN-GW.

### STEP 5

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 6

The Target BS initiates a CMAC Key Count Update procedure with the Authenticator ASN-GW to update it with the latest CMAC Key Count. See section 4.12 for this procedure.

### STEP 7

Upon completion of network entry, the target BS SHALL send a *HO\_Complete* message to the serving BS to acknowledge the completion of the handover. Relay ASN-GW relays the message over R4/R6 and starts timer  $T_{R4\_HO\_Comp}$ . Upon receipt of the *HO\_Complete* message, the Serving BS SHALL release the MS context and starts timer  $T_{R6\_HO\_Comp}$ .

### STEP 8

The Serving BS sends a *HO\_Ack* message to the Target BS. Relay ASN-GW relays the message over R4/R6 and stops timer  $T_{R4\_HO\_Comp}$ . Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Comp}$ .

### STEP 9

The Serving BS may have already sent the *HO\_Cnf* message with the *HO\_Indication* type set to "Cancel" to some or all Target BSs. For all unselected Target BSs to which such message has not been sent yet, the Serving BS SHALL send such a message upon receipt of *HO\_Complete* message in order to clear the MS context at target BSs. Relay ASN-GW relays the message over R4/R6. When Serving BS sends *HO\_Cnf* message it starts timer  $T_{R6\_HO\_Conf}$ .

### STEP 10

The unselected Target BS sends a *HO\_Ack* message to the Serving BS. Relay ASN-GW relays the message over R4/R6. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Conf}$ .

## STEP 11

Upon receiving the HO\_Complete message, if the Serving BS still has a data path with Anchor ASN-GW, the Serving BS SHALL initiate a Data Path De-Registration procedure with the Anchor ASN-GW. See section 4.1.3 for this procedure. Upon completing the Data Path Registration procedure with the Target BS, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure with the old Serving BS. Note: This step may occur any time after step '4'. Also if pre-established during HO preparation stage, the Anchor ASN-GW SHALL de-register all the pre-registered data paths with the other (not selected) Target BSs.

### 4.7.4 HO and Scanning Control for Fixed/Nomadic SS/MS

In [11], Neighbor list of BSs are advertised through broadcast message, MOB\_NBR-ADV, and all MSs whether Fixed/Nomadic or Full mobility SS/MS see this message. An MS whether designated with a Fixed, Nomadic or Full mobility class, is essentially the same in its PHY and MAC layers and procedures. Hence a Fixed/Nomadic MS, when it sees the over the air advertised Neighbor list of MSs, starts scanning like an unrestricted MS and if the RF conditions are suitable, generates a Handoff request at the current serving BS, to the new target BS. Since Fixed/Nomadic MS has restricted mobility, this scanning may generate a lot of spurious handoff requests to non-allowed target BSs, when RF thresholds are met. To limit this spurious handoff requests, the MS scanning may be controlled, when it makes requests for scanning durations by MOB\_SCN-REQ. A general call flow is given below.

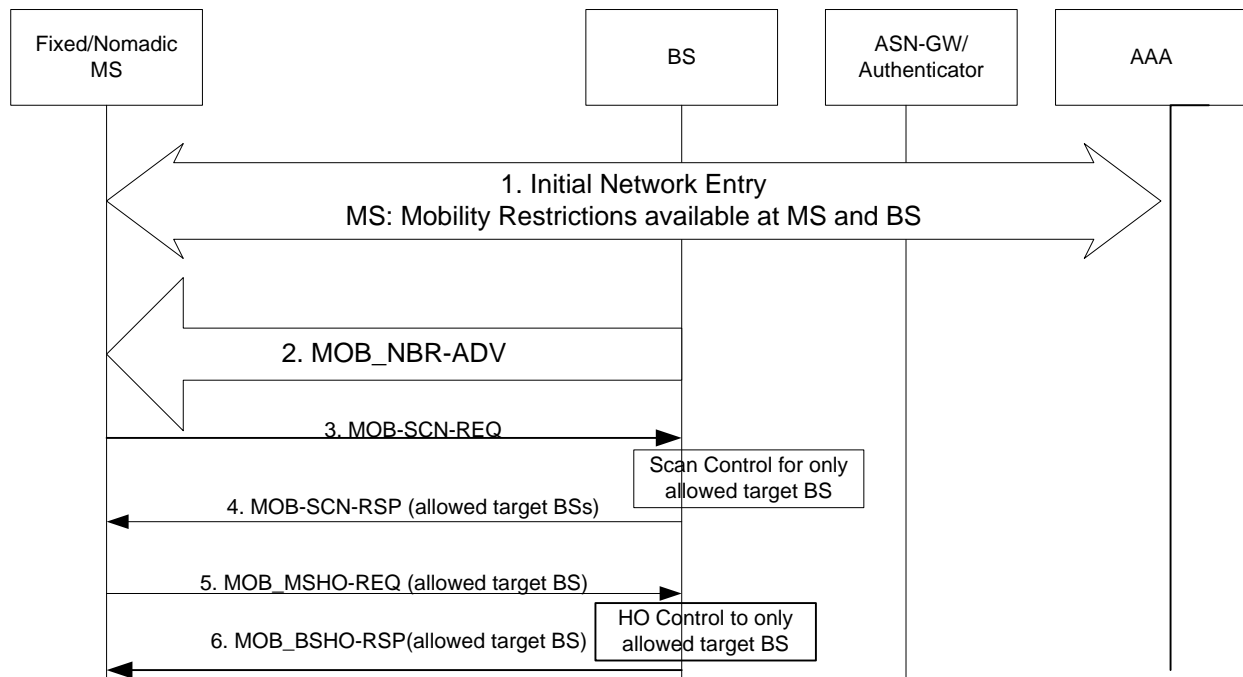


Figure 4-93 – HO and Scanning Control for Fixed/Nomadic SS/MS

## STEP 1

Initial Network Entry as described in section 4.5 and Figure 4-51. SS/MS's Fixed Nomadic restrictions are known to Authenticator as well as the Serving BS.

## STEP 2

BS performs default advertisement of its available target BSs to all MSs irrespective of their mobility class.

### STEP 3

Fixed/Nomadic MS makes request for scanning slots for all target BSs in the neighbor advertisement, MOB\_NBR-ADV message.

### STEP 4

BS recognizes the Fixed/Nomadic restriction of the SS/MS and does scanning control to only allowed target BSs as specified in the Reattachment zone list. It prunes the allowed scanning targets and allocates scanning slots only for those targets and sends back MOB\_SCN-RSP. In the case of Fixed SS/MS this list may be zero.

### STEP 5

When RF conditions and thresholds are met, SS/MS makes handoff request to serving BS with allowed BSs as its target.

### STEP 6

Serving BS, receives the handoff request. It checks and performs handoff control based on the mobility restrictions applicable for the particular MS and sends MOB\_BSHO-RSP back.

## 4.7.5 Message Definitions for HO Preparation Phase

### 4.7.5.1 Message Definitions for HO Preparation Phase

This section describes the R4 message definitions for the HO Preparation Phase.

**Table 4-82 – HO\_Req**

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	
Registration Type	5.3.2.145	O	This SHALL be included when Data Path Pre-reg is piggybacked. TC bit SHALL be set to 1.If the Target BS does not support combining of Data Path Control and HO Control message, it ignores this TLV.
MS Info	5.3.2.103	M	
>NSP ID	5.3.2.368	O	NSP identifier. Used to help distinguish the R4 and R6 tunnels for a specific NSP.
>Anchor ASN GW ID	5.3.2.10	M	Identifies the node that hosts the Anchor DP Function in the Anchor ASN.
>Authenticator ID	5.3.2.19	M	Identifies the node that hosts Authenticator and Key Distributor Function. Included if the security context is not included in the message.
>Anchor MM Context	5.3.2.11	O	The TLV MAY be included in order to optimize FA Relocation to the Target ASN-GW after HO. If included, notifies the Target ASN-GW that FA relocation to the Target ASN-GW will be initiated after HO.
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.

IE	Reference	M/O	Notes
>SBC Context	5.3.2.174	O <sup>1</sup>	802.16e related MS session context.
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and DL management connections. If TLV is missing, HARQ is not used on management connections.
>>>HARQ Channel Mapping	5.3.2.455	O	Indicates one or more HARQ channel numbers that may be used for management connections. If TLV is not present then all HARQ channels can be used by management connections.
>>>PDU SN extended subheader for HARQ reordering	5.3.2.456	O	Specifies if PDU SN extended subheader and PDU ordering should be used for management connections. If TLV is not present then PDU SN is not used by management connections
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Supported Security Associations	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>MAC Mode	5.3.2.323	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of UL HARQ Channel	5.3.2.331	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of DL HARQ Channels	5.3.2.334	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Support	5.3.2.336	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator for MIMO Support	5.3.2.343	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>REG Context	5.3.2.144	O <sup>1</sup>	802.16e related MS session context.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per Frame Support	5.3.2.296	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	

IE	Reference	M/O	Notes
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>SA Descriptor (one or more)	5.3.2.170	O <sup>1</sup>	SHOULD be included by Serving ASN for the Target ASN.
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.

IE	Reference	M/O	Notes
>Mobility Access Classifier	5.3.2.423	O	Indicates the mobility access classification of the subscriber (fixed or Nomadic). It Shall be included if BS supports Mobility Restriction for stationary access and the MS mobility access classifier is known at the BS.
>Reattachment Zone	5.3.2.424	O	Indicates the list of BS IDs allowed for reattachment. Included if Mobility Access Classifier is included.
>SF Info (one or more)	5.3.2.185	M	
>>SFID	5.3.2.184	M	
>>Direction	5.3.2.59	M	
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and DL management connections. If TLV is missing, HARQ is not used on management connections.
>>>HARQ Channel Mapping	5.3.2.455	O	Indicates one or more HARQ channel numbers that may be used for management connections. If TLV is not present then all HARQ channels can be used by management connections.
>>>PDU SN extended subheader for HARQ reordering	5.3.2.456	O	Specifies if PDU SN extended subheader and PDU ordering should be used for management connections. If TLV is not present then PDU SN is not used by management connections
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.
>>ARQ Context	5.3.2.344	O	Contains ARQ related information of the service flow. This context is Mandatory when ARQ enable is set to 1.
>>>ARQ WINDOW SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.
>>>ARQ RETRY TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ RETRY TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ BLOCK LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ SYNC LOSS TIMEOUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ DELIVER IN ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ RX PURGE TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.



IE	Reference	M/O	Notes
>>>ARQ BLOCK SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>RECEIVER ARQ ACK PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>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 if the Serving ASN-GW is collocated with the Anchor ASN-GW. TC bit SHALL be set to 1. If the Target BS does not support combining of Data Path Control and HO Control message, it ignores this TLV as well as its child TLV(s).
>>>Data Path ID	5.3.2.44	CM	This TLV SHALL be included if Data Path Info is included in the transmitted message.
>>>Tunnel Endpoint	5.3.2.194	O	
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	M	The TLV SHALL be included if the R4 Tunneling Granularity is not per-SF.
>>>Classification Rule Index	5.3.2.30	M	Index assigned to the Packet Classification Rule.
>>> Classification Rule Priority	5.3.2.32	M	
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>> DSCP	5.3.2.409	O	TC bit set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV SHALL be included if BTS Data Delivery Service is included in the transmitted message.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.

IE	Reference	M/O	Notes
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>> Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.

IE	Reference	M/O	Notes
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>Media Flow Type	5.3.2.94	O	
>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>Reduced Resources Code	5.3.2.237	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.

IE	Reference	M/O	Notes
>>>PHS Rule Action	5.3.2.128	M	Mandatory if PHS-Rules are present.
BS Info (Serving)	5.3.2.26	M	
>BS ID	5.3.2.25	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.
>Round Trip Delay	5.3.2.156	O	MAY be included in order to allow the Target ASN, when receiving the HO_Req message, 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.
> Time Stamp	5.3.2.358	O	HO Request transmission time from the SBS. MAY be included in order to allow the Target ASN to estimate the message propagation delay.
BS Info (Target, one or more)	5.3.2.26	M	
>BS ID	5.3.2.25	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>AK Context	5.3.2.6	O	This TLV MAY only be included if Serving ASN-GW and Authenticator ASN-GW are co-located. TC bit SHALL be set to 1. If the Target BS does not support combining of AK Context and HO Control message, it ignores this TLV as well as its child TLV(s).
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>Relative Delay	5.3.2.146	O	MAY be included in order to allow the Target BS 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 BS to estimate whether the MS can receive the same quality of service as in the Serving BS.

IE	Reference	M/O	Notes
>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.
Certified-MS-Feature-List-For-GW	5.3.2.171	O <sup>2</sup>	List of MS Certified features for the GW
Certified-MS-Feature-List-For-BS	5.3.2.183	O <sup>3</sup>	List of MS Certified features for the BS

Note <sup>1</sup> : This TLV SHALL be included either in HO\_Req or in HO\_Cnf message.

Note <sup>2</sup> : This TLV SHALL be present if Certified-MS-Feature-List-for-GW is received as part of RADIUS/DIAMETER message.

Note <sup>3</sup> : This TLV SHALL be present if Certified-MS-Feature-List-for-BS is received as part of RADIUS/DIAMETER message.

The Context\_Req that is sent from the Target ASN to the Authenticator ASN is shown on the Table 4-83.

**Table 4-83 – Context\_Req from Target BS to Authenticator ASN-GW**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Set to indicate retrieval of AK Context.
MS Info	5.3.2.103	M	
>Authenticator ID	5.3.2.19	M	
BS Info (Serving)	5.3.2.26	M	Included in order to allow the Authenticator to apply authorization policies depending on SBS.
> Serving/Target Indicator	5.3.2.182	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	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	

The Context\_Rpt sent from the Authenticator GW to the Target GW appears as shown on the Table 4-84:

**Table 4-84 – Context\_Rpt from Authenticator ASN-GW to Target BS**

IE	Description	M/O	Notes
Failure Indication	5.3.2.69	O	Request Success or request failure or partial response.
Context Purpose Indicator	5.3.2.36	M	Set to indicate that that the Report contains AK Context.
MS Info	5.3.2.103	O	
>Service Authorization Code	5.3.2.181	O	May be included to convey Authorization Policy to the Target BS.
BS Info (Target)	5.3.2.26	M	Note 1.

IE	Description	M/O	Notes
>BS ID	5.3.2.25	M	
> AK Context	5.3.2.6	M	
>>AK	5.3.2.5	M	
>>AK ID	5.3.2.7	M	
>>AK Lifetime	5.3.2.8	M	
>>AK SN	5.3.2.9	M	
>>CMAC_KEY_COUNT	5.3.2.34	M	
Result Code	5.3.2.154	O	Provide result status for this message. If the result status is any value other than 0, then this TLV SHALL be included. (Note 2).

Note 1: In both R6 and R4 handover messages, as well as on R8 handover message, only one target BS Info is contained.

Note 2: If the Authenticator ASN-GW supports context retrieval procedure only for 1 BS at a time, then it includes the context information for the first BS and it MAY include a result code with a value “Multiple not supported”.

If the Authenticator ASN-GW does not provide any context information, then it includes the result code with a value “Request Failure”.

If the Authenticator ASN-GW supports context retrieval procedure for multiple BS Info but provides context information for some BSs and not all BSs requested in the message, the Authenticator ASN-GW includes the context information for the BSs for which context is available and it SHOULD include a result code with the value “Partial Response”.

If the Authenticator ASN-GW does not provide any context information, then it includes the Failure Indication with a value “Request Failure”.

*HO\_Rsp* format is shown on the Table 4-85.

**Table 4-85 – HO\_Rsp**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
HO Type	5.3.2.79	M	
MS Info	5.3.2.103	M	
>SF Info (one or more)	5.3.2.185	M	It MAY be included if a) Target ASN suggests per SF QoS parameters different from those the Serving ASN has sent in <i>HO_Req</i> or b) the Target ASN needs to deliver per-SF Data Path Info.
>>SFID	5.3.2.184	M	
>> Reservation Result	5.3.2.152	M	

IE	Reference	M/O	Notes
>>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 if the Serving ASN-GW is collocated with the Anchor ASN-GW.  TC bit SHALL be set to 1.If the Target BS does not support combining of Data Path Control and HO Control message, it ignores this TLV as well as its child TLV(s).
>>>Data Path ID	5.3.2.44	CM	This TLV SHALL be included if Data Path Info is included in the transmitted message.
>>>Tunnel Endpoint	5.3.2.194	O	
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	5.3.2.182	M	Set to Serving.
>BS ID	5.3.2.25	M	
BS Info (Target)	5.3.2.26	M	Note 1.
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	
>BS HO RSP Code	5.3.2.203	O	0: VOID 1: Target BS doesn't support this HO Type; 2: Target BS rejects for other reasons; 3: Target BS's CPU overload; 4: Target BS rejects for other reasons; 5-255: Reserved.  This TLV SHALL be mandatory if multiple target BS Info TLVs are present and if one of the Target BS handover transaction.  If only one Target BS was included in the corresponding HO_Req, the failure SHALL be indicated in the Failure Indication TLV instead of this TLV and this TLV SHALL be omitted.
>HO ID	5.3.2.205	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 defaults to 3 (No Service Level Prediction 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.

IE	Reference	M/O	Notes
> HO Authorization Policy Support	5.3.2.367	O	The value has to be delivered to the MS with MOB_BSHO-RSP.
>Action Time	5.3.2.4	O	If not included defaults to 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. This value is defined in absolute number of airframes.
> Time Stamp	5.3.2.358	O	HO Response transmission time from the TBS. MAY be included in order to allow the Serving ASN to estimate the message propagation delay.
> 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	M	If only one target BS, SF Info could be described by the sub TLV of MS Info; If there are more than one Target BS, SF Info SHALL be described by the sub TLV of BS Info.
>>SFID	5.3.2.184	M	
>> Reservation Result	5.3.2.152	M	
Result Code	5.3.2.154	O	Provide result status for this message. If the result status is any value other than 0, then this TLV SHALL be included. (Note 1).

Note 1: In both on R6 and R4 handover messages, as well as on R8 handover message, only one target BS ID is contained.

Note 2: Both TLVs of Failure Indication and Result Code are optional, but one of them must be included in the message to indicate the result.

HO\_Ack format is shown on the Table 4-86:

**Table 4-86 – HO\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	
>Action Time	5.3.2.4	O	Number of frames where the TBS allocates a dedicated transmission opportunity for Fast Ranging. This SHALL be present only during the 3-way HO_Req/HO_Rsp/HO_Ack transaction. It SHALL not be present in the 2-way HO_Cnf/HO_Ack & HO_Complete/HO_Ack transactions.



IE	Reference	M/O	Notes
>Time Stamp	5.3.2.358	O	Transmission time for MOB_BSHO-REQ or MOB_BSHO-RSP over R1. May be included in order for the Target to estimate with greater accuracy when the fast ranging IE should be sent to the MS. This MAY be present only during the 3-way HO_Req/HO_Rsp/HO_Ack transaction. It SHALL not be present in the 2-way HO_Cnf/HO_Ack & HO_Complete/HO_Ack transactions.

1 The content of the *Path\_Prereg\_Req* is specified in the Table 4-87.

2 **Table 4-87 – Path\_Prereg\_Req**

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	O	MAY be omitted if the IP Destination (for Target Centric) or IP Source (for Anchor Centric) is the Anchor ASN-GW.
>SF Info (one or more)	5.3.2.185	M	It SHALL be included if the R4 Tunneling granularity is per SF.
>>SFID	5.3.2.184	M	
>>Direction	5.3.2.59	M	Specifies the direction of the reservation.
>>Data Delivery Trigger	5.3.2.265	O	Triggers data delivery for the specified service flow.
>>CID	5.3.2.29	O	It SHALL be included if the Anchor ASN allocates CID.
>>Data Path Info	5.3.2.45	O	Data Path which should be used for the service flow. Data Path Info TLV SHALL be Present only for the Service Flow which the Sender is responsible for creating.
>>>Data Path ID	5.3.2.44	CM	
>>>Tunnel Endpoint	5.3.2.194	O	
>>QoS Parameters	5.3.2.141	O	It MAY be included on R6 when the target ASN-GW is not the Anchor GW.
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	

3 The content of *Path\_Prereg\_Rsp* is shown on the Table 4-88.

**Table 4-88 – Path\_Prereg\_Rsp**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Registration Type	5.3.2.145	M	
Result Code	5.3.2.154	O	Result Code TLV SHALL be present in the case of a failure condition Enumerator. The values are: <ul style="list-style-type: none"> <li>0x01 = Failure – No resources</li> <li>0x02 = Failure – Not supported</li> </ul>
MS Info	5.3.2.103	M	
>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.
>SF Info (one or more)	5.3.2.185	M	It SHALL be included if the R4 Tunneling granularity is per SF.
>>SFID	5.3.2.184	M	
>>QoS Parameters	5.3.2.141	O	It MAY be included on R6 when the target ASN-GW is not the Anchor GW.
>>Data Delivery Trigger	5.3.2.265	O	Triggers data delivery for the specified service flow.
>>CID	5.3.2.29	O	
>>Data Path Info	5.3.2.45	O	Data Path which SHALL be used for the service flow. Data Path Info TLV SHALL be Present only for the Service Flow which the Sender is responsible for creating.
>>>Data Path ID	5.3.2.44	CM	
>>>Tunnel Endpoint	5.3.2.194	O	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	

The content of *Path\_Reg\_Ack* is shown on the Table 4-89.

**Table 4-89 – Path\_Prereg\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Registration Type	5.3.2.145	M	

#### 4.7.5.2 Message Definitions for HO Action Phase

This section describes the message definitions for the HO Action Phase.

1

**Table 4-90 – HO\_Cnf (HO Confirm Type is Confirm or Unconfirmed)**

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	
>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.
>Anchor MM Context	5.3.2.11	O	The TLV MAY be included, for Unconfirmed Type and to Targets that were not sent HO_Req during the Preparation phase, in order to optimize FA Relocation to the Target ASN-GW after HO. If included, notifies the Target ASN-GW that FA relocation to the Target ASN-GW will be initiated after successful HO.
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.
>SBC Context	5.3.2.174	O <sup>1</sup>	802.16e related MS session context.
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Supported Security Associations	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>MAC Mode	5.3.2.323	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of UL HARQ Channel	5.3.2.331	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of DL HARQ Channels	5.3.2.334	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Support	5.3.2.336	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Uplink Control Channel Support	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator for MIMO Support	5.3.2.343	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>REG Context	5.3.2.144	O <sup>1</sup>	802.16e related MS session context.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

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

IE	Reference	M/O	Notes
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>SA Descriptor	5.3.2.170	O <sup>1</sup>	SHOULD be included by Serving ASN for the Target ASN.
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.

IE	Reference	M/O	Notes
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>Mobility Access Classifier	5.3.2.423	O	Indicates the mobility access classification of the subscriber (fixed or Nomadic). It Shall be included if BS supports Mobility Restriction for stationary access and the MS mobility access classifier is known at the BS.
>Reattachment Zone	5.3.2.424	O	Indicates the list of BS IDs allowed for reattachment. It Shall be included when Mobility Access Classifier is included.
>SF Info (one or more)	5.3.2.185	M	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.
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	M	The TLV SHALL be included if the R4 Tunneling Granularity is not per-SF.
>>>Classification Rule Index	5.3.2.30	M	Index assigned to the Packet Classification Rule.
>>>Classification Rule Priority	5.3.2.32	M	
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>> DSCP	5.3.2.409	O	TC bit is set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.

IE	Reference	M/O	Notes
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV SHALL be included if BE Data Delivery Service is included in the transmitted message.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>> Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.



IE	Reference	M/O	Notes
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>Media Flow Type	5.3.2.94	O	
>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>Reduced Resources Code	5.3.2.237	O	
Refresh IP address trigger	5.3.2.375	O	Included for the BS to trigger IP address refresh on the MS via HO Process Optimization TLV Bit #13. Currently used only for Simple IP re-anchoring.
BS Info (Serving)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.
>BS ID	5.3.2.25	M	

IE	Reference	M/O	Notes
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	
>HO ID	5.3.2.205	O	MAY be included as optional reference if the Target ASN has previously sent it with <i>HO_Rsp</i> .
>AK Context	5.3.2.6	O	This TLV MAY only be included if Serving ASN-GW and Authenticator ASN-GW are co-located. TC bit SHALL be set to 1. If the Target BS does not support combining of AK Context and HO Control message, it ignores this TLV as well as its child TLV(s).
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.

1 Note <sup>1</sup> : This TLV SHALL be included either in HO\_Req or in HO\_Cnf message.

2 **Table 4-91 – HO\_Cnf (HO Confirm Type is Cancel or Reject)**

IE	Reference	M/O	Notes
HO Type	5.3.2.79	M	
HO Confirm Type	5.3.2.76	M	
BS Info (Serving)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.
>BS ID	5.3.2.25	M	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	
>HO ID	5.3.2.205	O	MAY be included as optional reference if the Target ASN has previously sent it with <i>HO_Rsp</i> .

3

4 The content of the *Context\_Req* from Target BS to Serving BS appears in Table 4-92.

**Table 4-92 – Context\_Req from Target BS to Serving BS**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Set to MAC Context Retrieval. Optionally, may include AK Context Retrieval as well.
BS Info (Serving)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.
>BS ID	5.3.2.25	M	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	

The content of the *Context\_Rpt* from the Serving BS to the Target BS appears in Table 4-93.

**Table 4-93 – Context\_Rpt from Serving BS to Target BS**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Context Purpose Indicator	5.3.2.36	M	Set to MAC Context Retrieval. Optionally, may include AK Context Retrieval as well.
MS Info	5.3.2.103	M	
>Service Authorization Code	5.3.2.181	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 <i>HO_Req</i> 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. Included if the originator of the <i>HO_Req</i> does not host the Authenticator and Key Distributor Function for the MS.
>SBC Context	5.3.2.174	O	802.16e related MS session context.
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and DL management connections. If TLV is missing, HARQ is not used on management connections.
>>>HARQ Channel Mapping	5.3.2.455	O	Indicates one or more HARQ channel numbers that may be used for management connections. If TLV is not present then all HARQ channels can be used by management connections.

IE	Reference	M/O	Notes
>>>PDU SN extended subheader for HARQ reordering	5.3.2.456	O	Specifies if PDU SN extended subheader and PDU ordering should be used for management connections. If TLV is not present then PDU SN is not used by management connections
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Supported Security Associations	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>MAC Mode	5.3.2.323	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of UL HARQ Channel	5.3.2.331	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of DL HARQ Channels	5.3.2.334	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Support	5.3.2.336	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator for MIMO Support	5.3.2.343	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>REG Context	5.3.2.144	O	802.16e related MS session context.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per Frame Support	5.3.2.296	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>SA Descriptor (one or more)	5.3.2.170	O	SHOULD be included by Serving ASN for the Target ASN.
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>Mobility Access Classifier	5.3.2.423	O	Indicates the mobility access classification of the subscriber (fixed or Nomadic). It Shall be included if BS supports Mobility Restriction for stationary access and the MS mobility access classifier is known at the BS.
>Reattachment Zone	5.3.2.424	O	Indicates the list of BS IDs allowed for reattachment. It Shall be included when Mobility Access Classifier is included.

IE	Reference	M/O	Notes
>SF Info (one or more)	5.3.2.185	M	It is included if TEK or Data Integrity information needs to be delivered. This TLV SHALL be included for uncontrolled handover.
>>SFID	5.3.2.184	M	
>>Direction	5.3.2.59	M	Specifies the direction of the flow.
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and DL management connections. If TLV is missing, HARQ is not used on management connections.
>>>HARQ Channel Mapping	5.3.2.455	O	Indicates one or more HARQ channel numbers that may be used for management connections. If TLV is not present then all HARQ channels can be used by management connections.
>>>PDU SN extended subheader for HARQ reordering	5.3.2.456	O	Specifies if PDU SN extended subheader and PDU ordering should be used for management connections. If TLV is not present then PDU SN is not used by management connections
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.
>>ARQ Context	5.3.2.344	O	Contains ARQ related information of the service flow. This context is Mandatory when ARQ enable is set to 1.
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_SYNC_LOSS_TIME OUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RX_PURGE_TIMEO UT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>RECEIVER_ARQ_ACK_P ROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.



IE	Reference	M/O	Notes
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	The TLV SHALL be included if the R4 Tunneling Granularity is not per-SF.
>>>Classification Rule Index	5.3.2.30	CM	This TLV SHALL be included if Packet Classification Rule / Media Flow Description is included in the transmitted message. Index assigned to the Packet Classification Rule.
>>>Classification Rule Priority	5.3.2.32	O	
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>> DSCP	5.3.2.409	O	TC bit set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV SHALL be included if BE Data Delivery Service is included in the transmitted message.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.

IE	Reference	M/O	Notes
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>> Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.

IE	Reference	M/O	Notes
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>Media Flow Type	5.3.2.94	O	
>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>Reduced Resources Code	5.3.2.237	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHS Rule Action	5.3.2.128	CM	Mandatory if PHS-Rules are present.
BS Info (Serving)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.
>BS ID	5.3.2.25	M	
BS Info (Target)	5.3.2.26	M	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
>BS ID	5.3.2.25	M	
>AK Context	5.3.2.6	O	

IE	Reference	M/O	Notes
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.

1 The content of *Path\_Reg\_Req* is shown in Table 4-94. 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 4-94 – Path\_Reg\_Req**

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	O	MAY be omitted if the IP Destination is Anchor ASN-GW. Otherwise, it SHALL be included.
>SF Info (one or more)	5.3.2.185	M	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	Data Path which SHALL be used for the service flow. Data Path Info TLV SHALL be Present only for the Service Flow which the Sender is responsible for creating.
>>>>Data Path ID	5.3.2.44	CM	
>>>>Tunnel Endpoint	5.3.2.194	O	
BS Info (Target)	5.3.2.26	M	SHALL be included to provide reference to the Target BS.
>BS ID	5.3.2.25	M	

4 The content of *Path\_Reg\_Rsp* is shown in Table 4-95. If Pre-Registration took place prior to Registration, none of  
5 the optional TLVs specified below needs to be included in the message.

6 **Table 4-95 – Path\_Reg\_Rsp**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

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	O	MAY be omitted if the IP Source is Anchor ASN-GW. Otherwise, it SHALL be included.
>SF Info (one or more)	5.3.2.185	M	R4 Tunneling granularity is per SF.
>>SFID	5.3.2.184	M	
>>Data Path Info	5.3.2.45	O	Data Path which SHALL be used for the service flow. Data Path Info TLV SHALL be Present only for the Service Flow which the Sender is responsible for creating.
>>>Data Path ID	5.3.2.44	CM	
>>>Tunnel Endpoint	5.3.2.194	O	
>>SDU Info	5.3.2.176	O	
>>>SDU SN	5.3.2.178	CM	
BS Info (Target)	5.3.2.26	M	
>BS ID	5.3.2.25	M	

1  
2 The content of *Path\_Reg\_Ack* is shown in Table 4-96.

3 **Table 4-96 – Path\_Reg\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

4  
5 The content of the *CMAC\_Key\_Count\_Update* appears in Table 4-97.

6 **Table 4-97 – 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.
> CMAC_KEY_COUNT	5.3.2.34	M	Delivers the CMACv2 Counter to the Authenticator.
>Authenticator ID	5.3.2.19	M	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	
Idle Mode Exit Indicator	5.3.2.369	O	This SHALL be included during Idle Mode Exit procedure.

7

The content of CMAC\_Key\_Count\_Update\_Ack is shown in Table 4-98.

**Table 4-98 – CMAC\_Key\_Count\_Update\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
MS Info	5.3.2.103	M	
>Authenticator ID	5.3.2.19	M	Authenticator ID for the MS.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

The content of the HO Complete from selected Target ASN to Serving ASN appears in Table 4-99.

**Table 4-99 – 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	
> Serving/Target Indicator	5.3.2.182	M	Set to Target.
> BS ID	5.3.2.25	M	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. Mandatory only if sub-TLVs are present.
>SF Info	5.3.2.185	O	
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.
>>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	CM	Last transmitted SDU sequence number. This TLV SHALL be included if SDU Info is included in the transmitted message

#### 4.7.6 ASN Anchored Mobility Scenarios Over R8 and R6

This section discusses ASN Anchored mobility scenarios over R8 and R6. The ASN consists of Distribution Function for the MS located with the serving BS at the same ASN which convey both data and signaling information. The BSs SHALL be connected to the ASN GWs with R6 interfaces. The neighboring BSs within the ASN MAY be interconnected with R8 interface for signaling between them. The ASN GWs SHALL be interconnected with R4 interfaces for signaling as well as data. This section discusses ASN anchored mobility scenarios with signaling over R6 or R8 between the Serving BS and the Target BSs that reside in the same ASN and corresponding datapath establishment procedures over R6. R4 operations, if executed, are identical to those described in section 4.7.2. Figure-6-1 in stage 2, section 6.1 shows the relevant network interfaces.

With respect to R6 and R8 operations the entities that participate in HO process are logically divided into the following types:

- a. Serving BS that hosts Serving HO Function and serves the MS prior to HO.
- b. Target BS that hosts Target HO Function. There might be one or more Target BSs. One of them is selected as the final HO Target and becomes Serving BS after HO completion.
- c. Anchor ASN GW that hosts the Anchor DP Function for the MS. Serving ASN GW MAY be located on the path between Anchor ASN GW and Serving BS. Target BS GW MAY be located on the path between the Anchor ASN GW and Target BS. In this case each such Data Path has R6 segment and R4 segment. Since this section discusses only R6 and R8 operations, it is assumed in the text below that the Data Path between BSs and the Anchor GW goes directly over R6. In other words the BS and the Anchor GW reside at the same ASN
- d. Authenticator ASN GW that hosts Authenticator/Key Distributor Function for the MS."
- e. If R8 is not supported, or the Target BS is located in a different ASN, the Hand Over messages (i.e. HO\_Req, HO\_Rsp, HO\_Ack, HO\_Cnf, HO\_Complete) are sent over R6 through at least one Relay ASN-GW. In such case a single HO\_Req is generated for every candidate Target BS and sent over R6 through the Relay ASN-GW.

Data integrity may be optionally applied during the HO procedure to minimize or prevent data loss as a result of the HO.

#### **4.7.6.1 Fully Controlled HO**

##### **4.7.6.1.1 HO Preparation Phase**

Upon receipt of a MOB-MSHO\_REQ message from a mobile station (MS), or upon a decision to instigate Network Initiated HO, the Serving BS SHALL initiate a handover to one or more candidate Target BSs by sending a HO\_Req(s) message to the Target BS(s) over the R8 interface(s).

The HO\_Req message SHALL contain an Authenticator ID TLV that points to the Authenticator/Key Distributor Function hosted in the Authenticator ASN GW. Thus upon receiving a HO\_Req message, the Target BS(s) MAY retrieve AK Context and Service Authorization Info TLV from the Authenticator ASN GW. The Target BS(s) is/are not required to retrieve this information immediately upon receipt of the HO Req message and MAY postpone the retrieval until the Handover Action Phase. This call flow scenario (subsequently referred to as Scenario 1) is shown in Figure 4-94.

Alternatively, the Serving BS MAY request on behalf of the target BS the AK Context from the Authenticator ASN and include it in the HO\_Req message

After receiving the HO\_Req message, each Target BS MAY pre-establish the data path for the MS with the Anchor ASN GW, if the HO\_Req message includes the Anchor ASN GW ID TLV which points to the ASN GW that hosts the Anchor DP Function. Data Path Pre-Registration at the Handover Preparation Phase is optional and may be executed only when all entities involved support this functionality. If the Anchor ASN GW does not support Data Path Pre-Registration and the Target BS attempts to initiate Data Path Pre-Registration procedure, the transaction should be rejected (i.e. Path\_Prereg\_Rsp message with a rejection code TLV will be sent back to the Target BS).

The Target BS SHALL respond to the HO\_Req message with the HO\_Rsp message, and the Serving BS SHALL acknowledge the Handover Preparation transaction completion by sending an HO\_Ack message back to the Target BS(s).

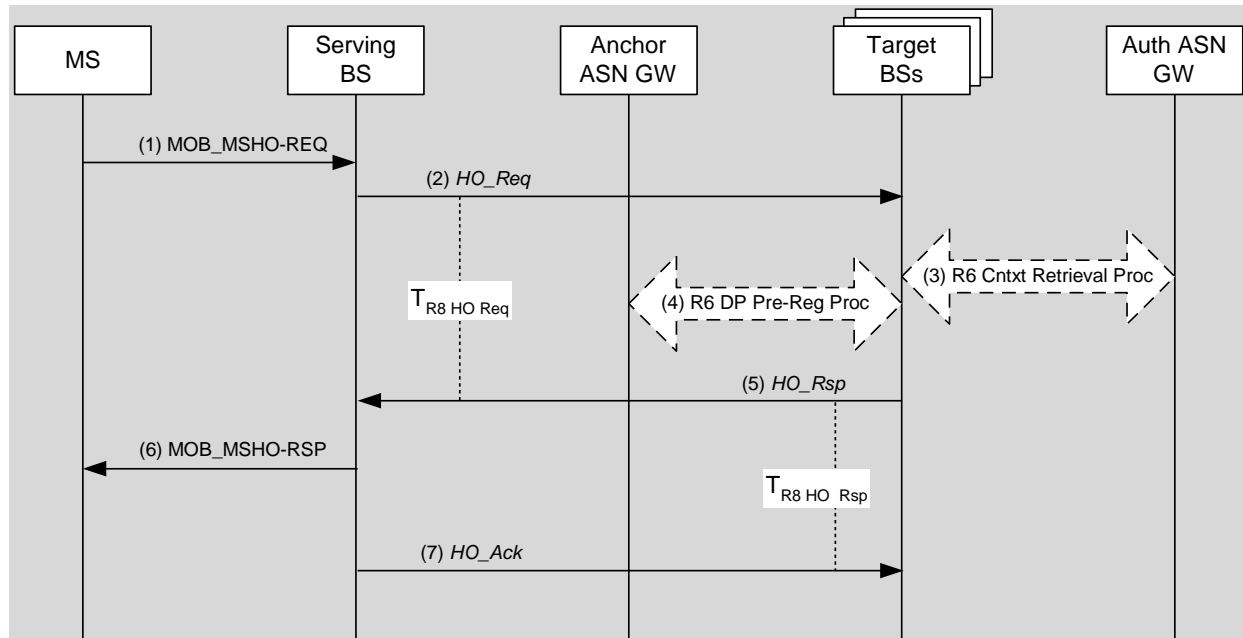
##### **4.7.6.1.1.1 R6 Data Path Pre-Registration Procedure**

The procedure is identical to the one described in 4.12.1.2.

##### **4.7.6.1.1.2 R6 Authenticator Context Retrieval Procedure**

The procedure is identical to the one described in 4.12.2.2.

##### **4.7.6.1.1.3 MS Initiated HO Preparation**



**Figure 4-94 – Successful MS Initiated HO Preparation**

### STEP 1

The MS initiates a handover by sending a MOB\_MSHO-REQ message to the Serving BS, which may include one or more potential target BS's.

### STEP 2

The Serving BS sends a *HO\_Req* message destined to each potential Target BS's selected for the handover and starts timer  $T_{R8-HO\_Req}$  or  $T_{R6-HO\_Req}$  respectively for each message. The message includes an Authenticator GW 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, of the candidate MS.

A Serving BS SHALL silently discard a duplicate MOB\_MSHO-REQ from an MS, if it has already initiated a HO preparation phase for this MS which is still ongoing. If a Serving BS receives such duplicate MOB\_MSHO-REQ from an MS, it SHALL not propagate the request further in to the network.

### STEP 3

Upon receipt of the *HO\_Req* message, the target BS(s) MAY request AK context and service authorization information for the MS by initiating a Context Retrieval procedure with the Authenticator ASN GW. Note: The Target BS(s) may optionally choose to defer this procedure to the Handover Action phase.

### STEP 4

The Target BS(s) MAY initiate pre-establishment of a data path for the MS with the Anchor ASN GW. If the Anchor ASN GW does not support the Data Path Pre-Registration, the *R6 Path\_Prereg\_Req* message from the Target BS will be responded by the *R6 Path\_Prereg\_Rsp* message with an appropriate reject cause code. Note: The Target BS(s) may optionally choose to defer this procedure to the handover Action Phase.

### STEP 5

The Target BS(s) sends a *HO\_Rsp* message to the Serving BS to acknowledge the handover request and starts timer  $T_{R8-HO\_Rsp}$  or  $T_{R6-HO\_Rsp}$  respectively. Upon receipt of the *HO\_Rsp* message, the Serving BS stops timer  $T_{R8-HO\_Req}$  or  $T_{R6-HO\_Req}$  respectively.



## STEP 6

The Serving BS sends a MOB\_BSHO-RSP message to the MS containing one or more potential target BS's selected by the Serving BS for the MS to handover to.

## STEP 7

The Serving BS sends a *HO\_Ack* message to the Target BS(s) controlling the potential target BS(s) selected for the MS. Upon receipt of the *HO\_Ack* message, the Target BS(s) stops timer  $T_{R8-HO\_Rsp}$  or  $T_{R6-HO\_Rsp}$  respectively.

### 4.7.6.1.1.4 Network Initiated HO Preparation

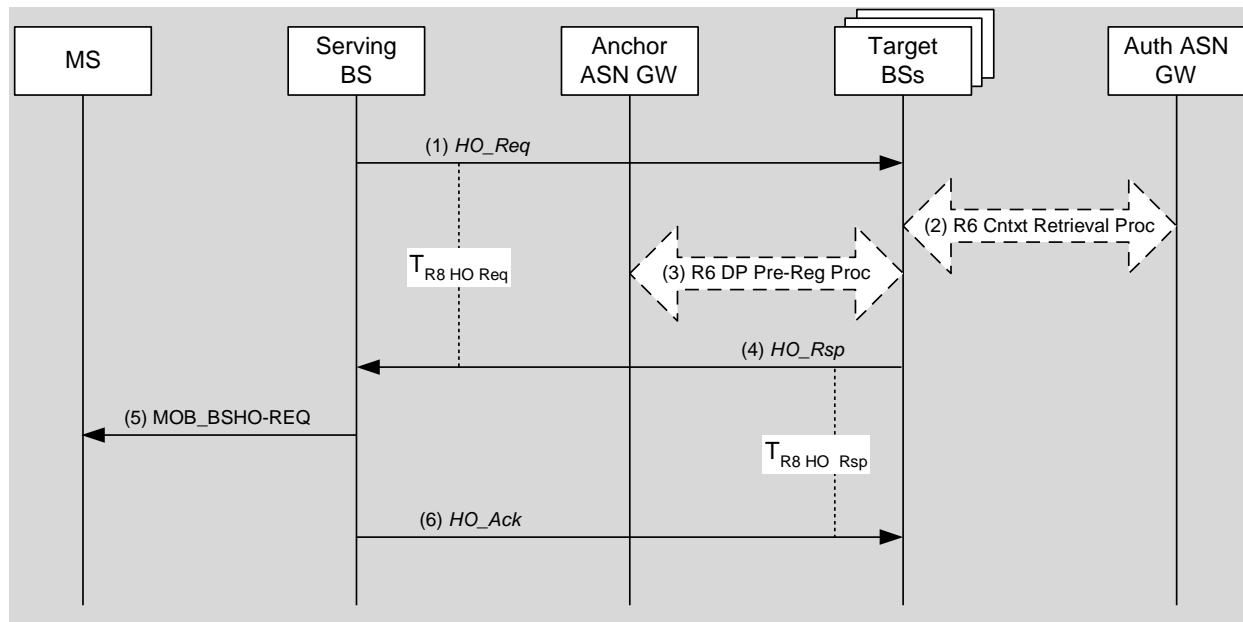


Figure 4-95 – Successful Network Initiated HO Preparation Phase

## STEP 1

The Serving BS initiates a handover by sending a *HO\_Req* message destined to each Target BS's selected for the handover and starts timer  $T_{R8-HO\_Req}$  or  $T_{R6-HO\_Req}$  respectively for each message. The message includes an Authenticator GW 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 2

The Target BS(s) requests AK context and service authorization information for the MS by initiating a Context Retrieval procedure with the Authenticator ASN GW. Note: The Target BS(s) may optionally choose to defer this procedure to the Handover Action phase.

## STEP 3

The Target BS(s) MAY initiate pre-establishment of a data path for the MS with the Anchor ASN GW. If the Anchor ASN does not support the Data Path Pre-Registration, the *R6 Path\_Prereg\_Req* message from the Target BS will be responded by the *R6 Path\_Prereg\_Rsp* message with an appropriate reject cause code. Note: The Target BS(s) may optionally choose to defer this procedure to the handover action phase.

## STEP 4

The Target BS(s) sends a *HO\_Rsp* message to the Serving BS to acknowledge the handover request and starts timer  $T_{R8-HO\_Rsp}$  or  $T_{R6-HO\_Rsp}$  respectively. Upon receipt of the *HO\_Rsp* message, the Serving BS stops timer  $T_{R8-HO\_Req}$  or  $T_{R6-HO\_Req}$  respectively.

## STEP 5

The Serving BS sends a MOB\_BSHO-REQ message to the MS containing one or more potential target BS's selected by the network for the MS to handover to.

## STEP 6

The Serving BS sends a *HO\_Ack* message to the Target BS(s) controlling the potential target BS(s) selected for the MS. Upon receipt of the *HO\_Ack* message, the Target BS(s) stops timer  $T_{R8-HO\_Rsp}$  or  $T_{R6-HO\_Rsp}$  respectively.

### 4.7.6.1.1.5 HO Preparation Stage Timers and Timing Considerations

This section identifies the timer entities participating in the HO Preparation Phase. The following timers are defined over R8:

- $T_{R8-HO\_Req}$ : is started by a Serving BS upon sending the *HO\_Req* message for an MS to a Target BS and is stopped upon receiving a corresponding *HO\_Rsp* message from the Target BS.
- $T_{R8-HO\_Rsp}$ : is started by a Target BS upon sending the *HO-Rsp* message for an MS to a Serving BS and is stopped upon receiving a corresponding *HO\_Ack* message from the Serving BS.

R6 Timers are identical to those defined in 4.7.2.1.6.

Table 4-100 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-100 – HO Preparation Phase Timer Values for HO messages over R8**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R8-HO\_Req}$	TBD		TBD
$T_{R8-HO\_Rsp}$	TBD		TBD

### 4.7.6.1.1.6 HO Preparation Stage Error Conditions

This section describes error conditions associated with the HO Preparation Phase.

#### 4.7.6.1.1.6.1 Timer Expiry

The following table shows details on 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 4-101.

**Table 4-101 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R8-HO\_Req}$	Serving BS	The Serving ASN may re-try HO to another Target BS. If no Target BS can be reached, the Serving BS SHALL send MS a MOB_BSHO-RSP with Mode set to 0b111
$T_{R8-HO\_Rsp}$	Target BS	No Action required

#### 4.7.6.1.1.6.2 HO\_Rsp Error

Upon receipt of the *HO\_Req* message, if the Target BS is unable to support the requested HO, then it SHALL send *HO\_Rsp* message with suitable error code included in the Result Code TLV. Upon receipt of the *HO\_Rsp* message indicating HO cannot be supported at a Target BS, the Serving BS SHALL stop  $T_{R8-HO\_Req}$  or  $T_{R6-HO\_Req}$  respectively (if running), and MAY re-send the *HO\_Req* message to a different Target BS. If the Serving BS does not re-send the

*HO\_Req* message, or if all subsequent Target BSs cannot support the HO, in the case of MS Initiated handover, the Serving BS SHALL send a *MOB\_BSHO\_RSP* with mode = 0b111: MS HO request not recommended (BS in list unavailable).

#### 4.7.6.1.2 HO Action Phase

The HO Action Phase begins when the MS leaves the Serving BS. The MS sends a *MOB\_HO-IND* message to the Serving BS in which it specifies which Target BS has been selected for the handover. 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 *MOB\_HO-IND*, the Serving BS SHALL generate a *HO\_Cnf* message and send it to the Target BS. The *HO\_Cnf* message includes the “most recent MAC context” at the Serving BS.

Upon receiving *HO\_Cnf* message with the HO Indication type whose value is not set to “Cancel”, or “Reject”, the Target BS SHALL retrieve the AK Context if this information was not retrieved during the Handover Preparation Phase. This call flow scenario (subsequently referred to as Scenario 1) is shown in Figure 4.

If the data path between the Anchor ASN GW and the Target BS was not pre-established at the Preparation Phase, it MAY be pre-established after receiving *HO\_Cnf* message and before the MS starts Network Re-Entry at the Target BS.

The data paths between the Anchor ASN GW and the Target BS SHALL be established via Data Path Registration procedure after the MS either starts or completes Network Re-Entry at the Target BS<sup>11</sup>. If Data Path Registration procedure is invoked after the data path had been pre-registered, the procedure only confirms final establishment of the pre-registered data paths and does not convey any parameters of the data paths except MS ID. In this case, all the parameters that are related to the data paths SHALL be exchanged during the preceding Data Path Pre-Registration transaction. Furthermore, the Data Path Registration transaction is completed with a two-way handshake; DP Registration Request and Response message exchange and no *Path\_Reg\_Ack* message (i.e. two-way handshake).

If no Data Path Pre-Registration procedure had been completed prior to the Data Path Registration procedure, the R6 *Path\_Reg\_Req* and *Path\_Reg\_Rsp* message SHALL convey all parameters relevant for the setup of Data Paths. In this case the R6 *Path\_Reg\_Ack* message SHALL be sent in response to R6 *Path\_Reg\_Rsp* message (i.e. three-way handshake).

Upon completion of Data Path Registration procedure, the Anchor ASN GW SHALL initiate de-registration of all the pre-registered data paths to the candidate Target BSs that have not been selected for the final handover target. Also, the Anchor ASN GW SHALL initiate de-registration of the data path between the (old) Serving BS and itself.

If the Serving BS determines that the *MOB\_HO\_IND* message was not received from the MS (due to a communication loss with the mobile<sup>12</sup>, or of the message was corrupted), for example upon expiration of internal timer<sup>13</sup>, the Serving BS MAY send the *HO\_Cnf* message; value for the HO Indication type should be set to an “Unconfirmed” which may include all “most recent MAC context”. Such *HO\_Cnf* message SHALL be sent to the set of Target BSs that were indicated in the previous *MOB\_BSHO-REQ* or *MOB\_BSHO-RSP* message that was sent by the Serving BS to the MS. The *HO\_Cnf* message may also be sent to target BSs which weren’t notified of a potential impending handover from the MS during the handover preparation phase and whose target BSs weren’t included in the *MOB\_BSHO-REQ* or *MOB\_BSHO-RSP* messages (e.g. candidate target BSs which were included in the *MOB\_MSHO-REQ* message sent by the MS but weren’t notified of the handover in the handover preparation phase). Upon sending the *HO\_Cnf* message to the candidate Target BS(s), the Serving BS SHALL stop all the downlink and uplink scheduling for the data transmission and reception from the MS respectively.

<sup>11</sup> If DP 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

<sup>12</sup> *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.

<sup>13</sup> For example,  $T_{MOB\_HO\_IND}$

Upon sending the *HO\_Cnf* message, if the Resource\_Retain flag was not set, the Serving BS SHALL discard all MS's connections resource information including the MAC state machine and all outstanding buffered PDUs, else the Serving BS SHALL retain the connections, MAC state machine and PDUs associated with the MS for service continuation until the expiration of Resource Retain Timer.

The Serving BS May release all MAC context and MAC PDUs associated with the MS upon reception of a *HO Complete* message from the Target BS indicating MS committed Network Attachment at the Target BS.

If the Target BS does not receive the *HO\_Cnf* message before the MS starts Network Reentry, the Target BS MAY request the "most recent MAC Context" via Context Request/Report exchange with the Serving BS as it is shown in Scenario 3.

Immediately after the MS completes Network Re-entry, the Target BS (which at that moment becomes new Serving BS) SHALL send *CMAC\_Key\_Count\_Update* message to the Authenticator over R6 or R6 and R4 to notify the successful HO completion at the selected Target BS. The message SHALL deliver to the Authenticator the value of the CMAC\_KEY\_COUNT which is received from the MS. For details of *CMAC\_Key\_Count\_Update*, refer to 4.3.4.2 Maintenance of CMAC Key Count by the Network. As soon as the MS Network Re-entry procedure at the Target BS is completed, the Target BS MAY send a *HO\_Complete* message to the Serving BS to expedite the resource release in the Serving BS.

#### 4.7.6.1.2.1 R6 Data Path Registration Procedure

For HO over R8, the procedure is identical to the one described in 4.12.3.1.

#### 4.7.6.1.2.2 R6 Data Path De-Registration Procedure

For HO over R8, the procedure is identical to the one described in 4.12.4.1

#### 4.7.6.1.2.3 CMAC Key Count Update Procedure

For HO over R8, the procedure is identical to the one described in 4.12.5.2.

#### 4.7.6.1.2.4 MAC Context Retrieval Procedure over R8

MAC Context Retrieval Procedure is shown in Figure 2:

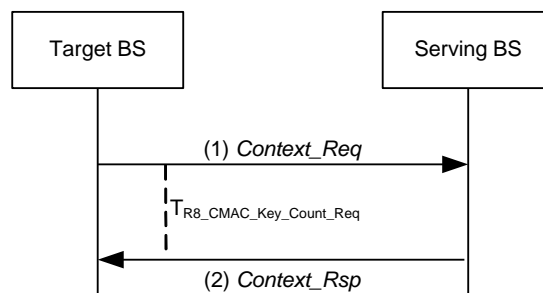


Figure 4-96 – MAC Context Retrieval Procedure

#### STEP 1

Target BS sends a *Context\_Req* message to request the context associated with a specified MS stored in the Serving BS. The Target BS starts timer  $T_{R8-Cntxt\_Req}$ .

#### STEP 2

Serving BS responds by sending the requested context information for the mobile in the *Context\_Rpt* message. Upon receipt of the *Context\_Rpt* message, Target BS stops timer  $T_{R8-Cntxt\_Req}$ .

#### 4.7.6.1.2.5 Handover Action Scenario 1: Serving BS Sends HO\_Cnf message After receiving MOB HO-IND

- 3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
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 Serving BS in the Handover Preparation phase HO\_IND\_type field in the message is set to 0b00 (Serving BS Release).

Upon reception of the MOB\_HO-IND the Serving BS sends a *HO\_Cnf* message and starts timer T<sub>R8-HO Confirm</sub> or T<sub>R6-HO Confirm</sub> respectively. Serving BS MAY also send HO\_Cnf message with the value of the HO\_Indication type set to “Cancel” to all unselected Target BS(s) and clear the MS context.

The Target BS sends a *HO\_Ack* message. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R8-HO}$  Confirm or  $T_{R6-HO}$  Confirm.

**STEP 4**

If AK context and service authorization information for the MS was not requested during the Handover Preparation phase, the Target BS requests AK context and service authorization information for the MS by initiating a Context Retrieval procedure with the Authenticator ASN. Otherwise, this step SHALL be skipped.

**STEP 5**

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 6**

The MS initiates network re-entry with the Target BS by sending RNG-REQ. Serving BSID is included in the message and bit #0 is set to 1.

**STEP 7**

The Target BS responds with RNG-RSP and the MS and the Target BS complete Network Reentry.

**STEP 8**

Target BS initiates Data Path Registration procedure with the Anchor ASN GW. This procedure MAY take place immediately after step 6.

**STEP 9**

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 10**

Upon completing the Data Path Registration procedure with the Target BS, the Anchor ASN GW MAY initiate Data Path De-Registration procedure with the old Serving BS. Also, the Anchor ASN GW de-registers all the pre-registered data paths with the other unselected Target BSs. See discussion in 7.3.3.1.2.8 for more details.

**STEP 11**

Upon completion of network re-entry, the Target BS sends a *HO\_Complete* message to notify the completion of the handover and starts timer  $T_{R8-HO\_Comp}$  or  $T_{R6-HO\_Comp}$  respectively. Upon receipt of the *HO\_Complete* message, the Serving BS releases the MS context. If the Serving BS still has a data path with Anchor ASN GW, the Serving BS initiates Data Path De-Registration procedure (see section 7.3.3.1.2.8) with the Anchor ASN GW.

**STEP 12**

The Serving BS sends a *HO\_Ack* message to the Target BS. Upon receipt of the *HO\_Ack* message, the Target BS stops timer  $T_{R8\_HO\_Comp}$  or  $T_{R6-HO\_Comp}$  respectively.

**STEP 13**

Upon receiving *HO\_Complete* message, if Serving BS did not send *HO\_Cnf* message with the value of the *HO\_Indication* type set to “Cancel” to all the unselected Target BS(s) in STEP 2, it sends *HO\_Cnf* message with the value of the *HO\_Indication* type set to “Cancel” to all unselected Target BS(s) to clear the MS context and starts timer  $T_{R8-HO\_Confirm}$  or  $T_{R6-HO\_Confirm}$  respectively.

**STEP 14**

Upon receipt of the *HO\_Cnf(Cancel)* message the unselected Target BS(S) clear the MS context. The Target BS sends the *HO\_Ack* message. Upon receipt of the *HO\_Ack* the Serving BS stops timer  $T_{R8-HO\_Confirm}$  or  $T_{R6-HO\_Confirm}$  respectively.

#### 4.7.6.1.2.6 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 HO-IND and sends the *HO\_Cnf* messages to the entire set of the Target BSs. See also section 4.7.6.1.2.7 HO Action Scenario 3.

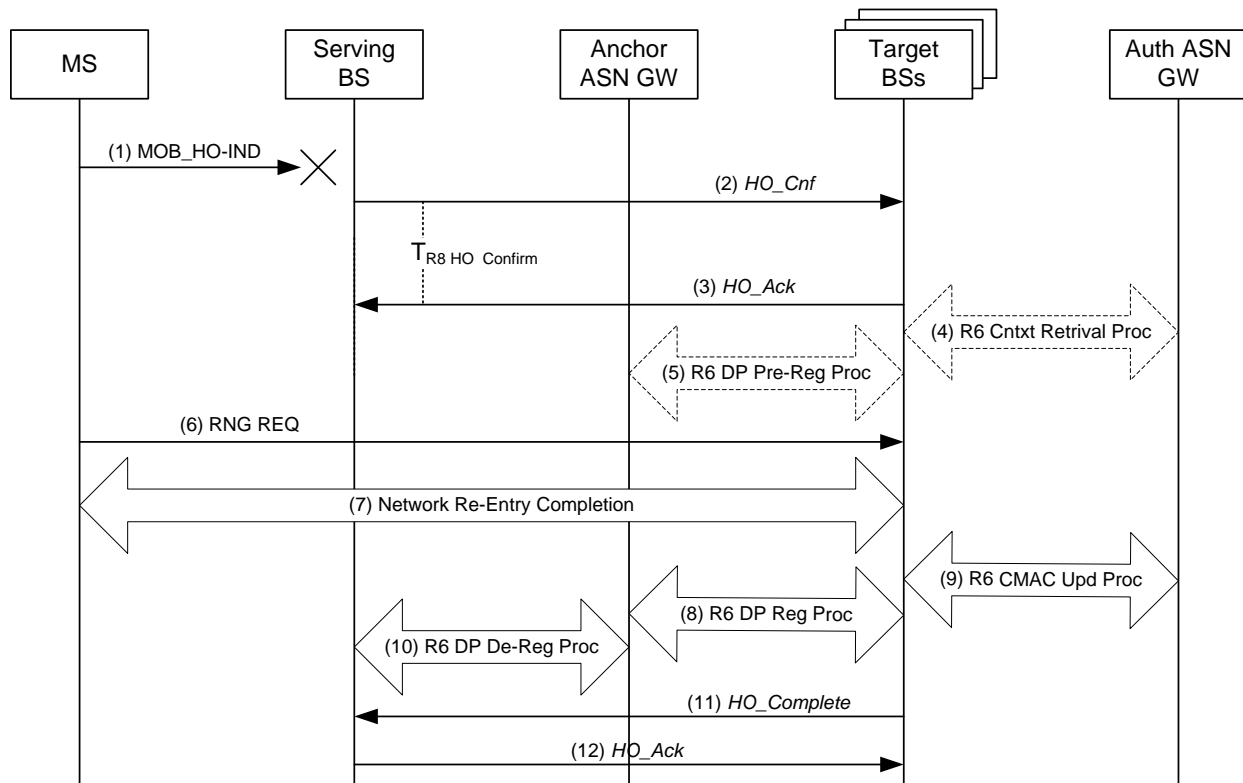


Figure 4-98 – Successful HO Action Phase, Scenario 2

The step description is the same as in Scenario 1 described in 4.7.6.1.2.5 with one difference – in this case in step 2, the serving BS sends multiple *HO\_Cnf* messages. The *HO\_Cnf* message may also be sent to candidate targets BSs the MS may chose to handover to which weren't previously notified of a potential handover from the MS during handover preparation. The *HO\_Cnf* message includes the HO\_Indication Type set to "Unconfirmed", and may include the most recent MAC content for the MS.

#### 4.7.6.1.2.7 Handover Action Scenario 3: Serving BS Doesn't Send R8 HO\_Cnf

The following call flow describes a successful Handover Action scenario where the MOB\_HO-IND sent by the MS to the Serving BS was lost over the air and not received by the Serving BS, and/or the HO\_Cnf message sent by the Serving BS to the Target BS was either delayed or not received. The MS completes network re-entry at one of the Target BSs selected by the Serving BS during the Handover Preparation phase.

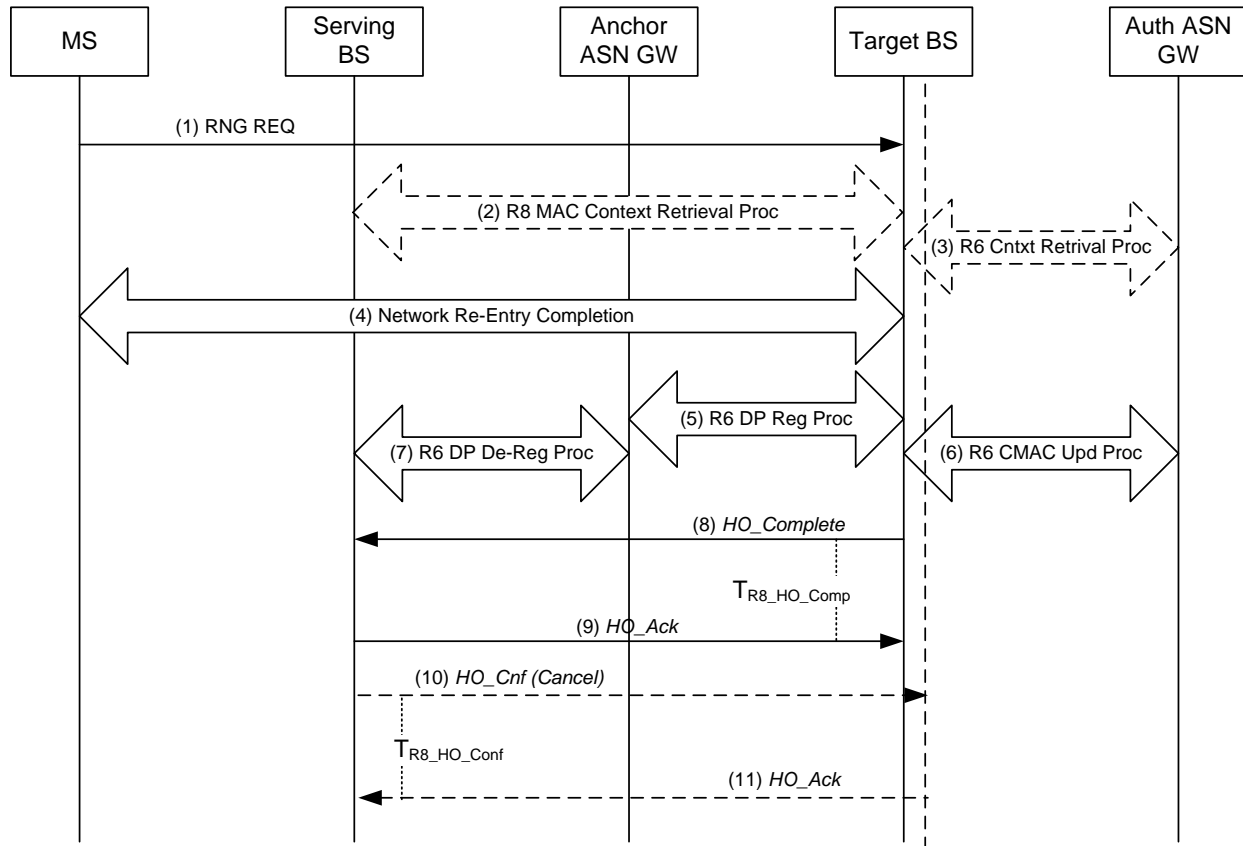


Figure 4-99 – Successful HO Action Phase, Scenario 3

#### STEP 1

The MS initiates network re-entry with the Target BS by sending RNG-REQ.

#### STEP 2

If the Target BS needs to synchronize the dynamic MAC context it initiates a Context Request procedure with the Serving BS to retrieve the latest MAC context for the MS.

#### STEP 3

If AK context and service authorization information was not obtained during the Handover Preparation phase, the Target BS requests AK context and service authorization information for the MS by initiating a Context Request procedure with the Authenticator ASN. This step might have been executed in the Preparation Phase and shown as optional in the Action Phase.

#### STEP 4

The Target BS responds with RNG-RSP and the MS and the Target BS complete Network Reentry.



**STEP 5**

Target BS initiates Data Path Registration procedure with the Anchor ASN GW. This procedure MAY take place immediately after step 3.

**STEP 6**

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 7**

Upon completing the Data Path Registration procedure with the Target BS, the Anchor ASN GW MAY initiate Data 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 unselected Target BSs. See discussion in 7.3.3.1.2.8 for more details.

**STEP 8**

Upon completion of network re-entry, the Target BS sends a *HO\_Complete* message to notify the completion of the handover. Upon receipt of the *HO\_Complete* message, the Serving BS releases the MS context and starts timer  $T_{R8\_HO\_Comp}$  or  $T_{R6-HO\_Comp}$  respectively. If the Serving BS still has a data path with Anchor ASN GW, the Serving BS initiates Data Path De-Registration procedure (see section 7.3.3.1.2.8) with the Anchor ASN GW.

**STEP 9**

The Serving BS sends a *HO\_Ack* message to the Target BS. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R8-HO\_Comp}$  or  $T_{R6-HO\_Comp}$  respectively.

**STEP 10**

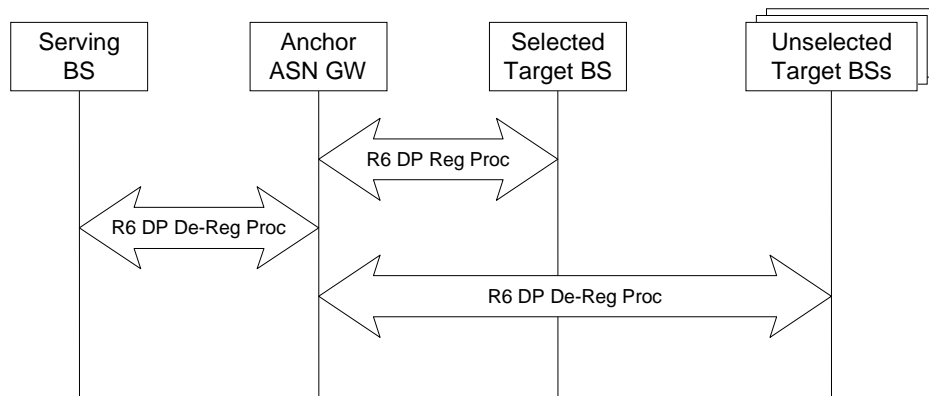
The serving BS may have already sent the *HO\_Cnf* message with the *HO\_Indication* type set to “Cancel” to some or all target BSs. For all unselected target BSs to which such message has not been sent yet, the serving BS sends such a message upon receipt of *HO\_Complete* message in order to clear the MS context at target BSs. When serving BS sends *HO\_Cnf* message it starts timer  $T_{R8\_HO\_Confirm}$  or  $T_{R6-HO\_Confirm}$  respectively.

**STEP 11**

Upon receipt of the *HO\_Cnf*(Cancel) message the Target BS(S) clear the MS context. The Target BS sends the *HO\_Ack* message. Upon receipt of the *HO\_Ack* message the Serving BS stops timer  $T_{R8-HO\_Confirm}$  or  $T_{R6-HO\_Confirm}$  respectively.

**4.7.6.1.2.8 Path De-Registration with Old Serving and Unselected Target BSs**

R6 Path Registration Procedure between the finally selected Target BS and Anchor ASN GW triggers R6 Path Deregistration of the Data Path between the Anchor ASN GW and the old Serving BS as well as between the Anchor ASN GW and each of the Unselected Target BSs. In the later case the procedure takes place if the corresponding Data Paths were previously pre-registered. The scenario is shown in Figure 4-100.



**Figure 4-100 – Path De-Registration with Old Serving and Unselected Target BSs**

All R6 Path Deregistration Procedures shown are independent of each other and may happen simultaneously.

#### 4.7.6.1.2.9 HO Action Phase Timers and Timing Considerations

This section identifies the timer entities participating in the HO Action Phase. The following timers are defined over R8:

- $T_{R8-HO\ Confirm}$ : is started by the Serving BS when sending a *HO\_Cnf* message to a Target BS, and is stopped upon receiving a *HO\_Ack* message from the corresponding Target BS.

R6 Timers are identical to those defined in 4.7.2.5.

Table 4-102 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-102 – HO Action Phase Timer Values for R8**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R8-HO\ Confirm}$	TBD		TBD
$T_{R8\_HO\_Comp}$	TBD		TBD

#### 4.7.6.1.2.10 HO Action Phase Error Conditions

This section describes error conditions associated with the HO Action Phase.

##### 4.7.6.1.2.10.1 Timer Expiry

The following table shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer expiry, if the maximum retries has not exceeded, the related message is retransmitted and the timer is restarted. Otherwise, the corresponding action(s) should be performed as indicated in Table 4-103.

**Table 4-103 – Timer Max retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R8-HO\ Confirm}$	(old) Serving BS	TBD

$T_{R8\_HO\_Comp}$	Target BS (New Serving)	No action required
--------------------	-------------------------	--------------------

#### 4.7.6.1.2.10.2 Context\_Rpt Error

Upon receipt of the *Context\_Req* message, if the Serving BS is unable to provide the requested information it SHALL send a *Context\_Rsp* message with the Reject Cause Code TLV to the sender of the *Context\_Req* message. Upon receipt of the *Context\_Rsp* message with Reject Cause Code TLV, the Target BS SHALL stop timer  $T_{R8\_Cntxt\_Req}$  or  $T_{R6\_Cntxt\_Req}$  respectively (if running), and MAY resend the *Context\_Req* message. If the Target BS does not resend the R8 *Context\_Req* message or if subsequent attempts are also unsuccessful, then the BS MAY send a *HO\_Rsp* message with suitable error code included in the Result Code TLV.

#### 4.7.6.1.3 HO Cancel

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 BS” below figures for various HO Cancellation scenarios is referred to the Target BS that was previously selected as the potential target BS that MS may handover to, and some system resource may have been pre-allocated at the target BS including the data path resources towards the anchor ASN.

##### 4.7.6.1.3.1 HO Cancellation Scenario 1: “Unselected BS” receives HO\_Cnf from Serving BS

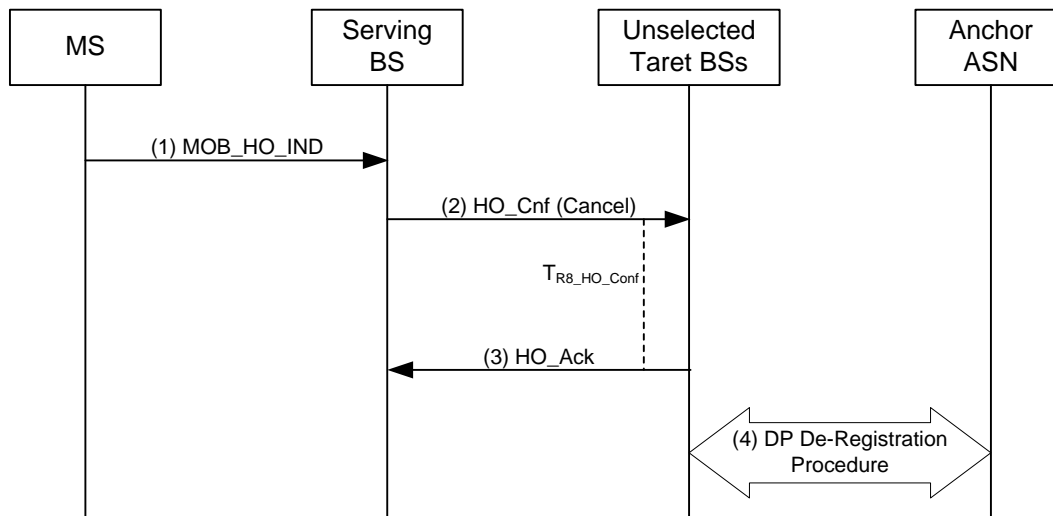


Figure 4-101 –HO Cancellation, Scenario 1

#### 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 *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 awaits *HO\_Ack* by starting the  $T_{HO\_Conf}$ . If the timer expires, the Serving BS may re-send the *HO\_Cnf*. After a pre-defined number of retransmissions, the Serving BS stops resending the *HO\_Cnf*. The Target BS SHALL perform the local clean up if *HO\_Cnf* is never received from the Serving BS.

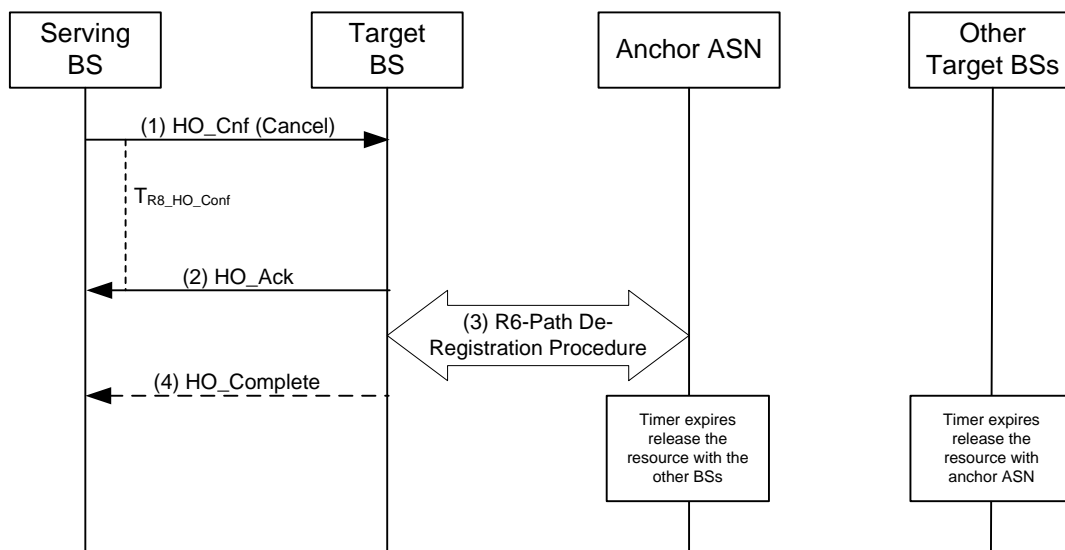
## STEP 3

Target BS receives the *HO\_Cnf* with HO\_Indication type set to “Cancel”. Target BS sends *HO\_Ack* to the Serving BS and may release the pre-allocated system resources, which are to support the MS handover. .

## STEP 4

The Target BS may send the *R6\_Path\_Dereg\_Req* to the Anchor ASN if data path has already been established between the Target BS and the Anchor ASN. Target BS sets the timer  $T_{R6\_Path\_Dereg\_Req}$  to wait for the response from the Anchor ASN. If the *R6\_Path\_DeReg\_Rsp* is not received by the Target BS before the expiry of the  $T_{R6\_Path\_Dereg\_Req}$ , the Target BS may re-transmit the message until the maximum number of retransmissions. If the MS is no longer attached to the Serving BS, the Serving BS SHALL release all the allocated system resource for the MS.

### 4.7.6.1.3.2 HO Cancellation Scenario 2: “Unselected BS does not Receive HO\_Cnf from Serving BS



**Figure 4-102 –HO Cancellation, Scenario 3**

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 1

Receiving the MOB\_HO-IND with HO\_IND\_type set to 0b01: HO Cancel causes the Serving BS to send *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 awaits

*HO\_Ack* by starting the  $T_{R8\_HO\_Conf}$  or  $T_{R6\_HO\_Conf}$  respectively. If the timer expires, the Serving BS may re-send the *HO\_Cnf*. After a pre-defined number of retransmissions, the Serving BS stops resending the *HO\_Cnf*. The Target BS SHALL perform the local clean up if *HO\_Cnf* is never received from the Serving BS.

## STEP 2

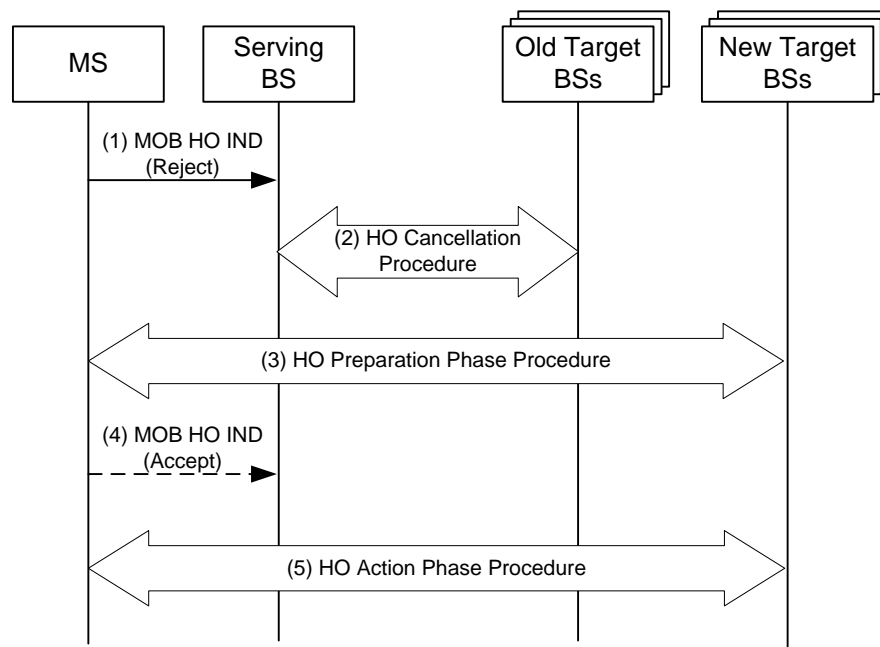
The Target BS does not receive the *HO\_Cnf*. Target BS releases the pre-allocated system resources which are to support the MS handover.

## STEP 3

After the timer associated with the pre-registered DP expires, the Target BS may send the *R6 Path\_Dereg\_Req* to the Anchor ASN if data path has already been established between the Target BS and the Anchor ASN. Target BS sets the timer  $T_{R6\_Path\_Dereg\_Req}$  to wait for the response from the Anchor ASN. If the *R6 Path\_DeReg\_Rsp* is not received by the Target BS before the expiry of the  $T_{R6\_Path\_Dereg\_Req}$ , the Target BS may re-transmit the message until the maximum number of retransmissions. . If the MS is no longer attached to the Serving BS, the Serving BS SHALL release all the allocated system resource for the MS.

### 4.7.6.1.4 HO Reject

The following call flow describes the scenario when the MS rejects target BSs offered to it by the serving BS for handover.



**Figure 4-103 – HO Reject**

1. The MS sends a MOB\_HO-IND containing HO\_IND\_Type TLV set to 0b10 indicating rejection of the target BS(s) offered by the serving BS for handover in the MOB\_BSHO-RSP (MS initiated handover) or MOB\_BSHO-REQ (network initiated handover) message.
2. The serving BS initiates the handover cancellation procedures described in section 4.7.2.3 with the target BS(s) which were rejected for handover by the MS.

The following steps only occur if the serving BS is able to offer an alternate target BS(s) to the MS.

3. The serving BS initiates the handover preparation procedure with a target BS(s) or through Relay ASN-GW(s) controlling a new candidate target BS(s) to be offered to the MS for handover.

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 BS completes the handover action procedures described in section 4.7.2.2 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 BS decides to offer a new target BS for handover to the MS, steps 3-5 are repeated.

#### 8       **4.7.6.2 Uncontrolled HO**

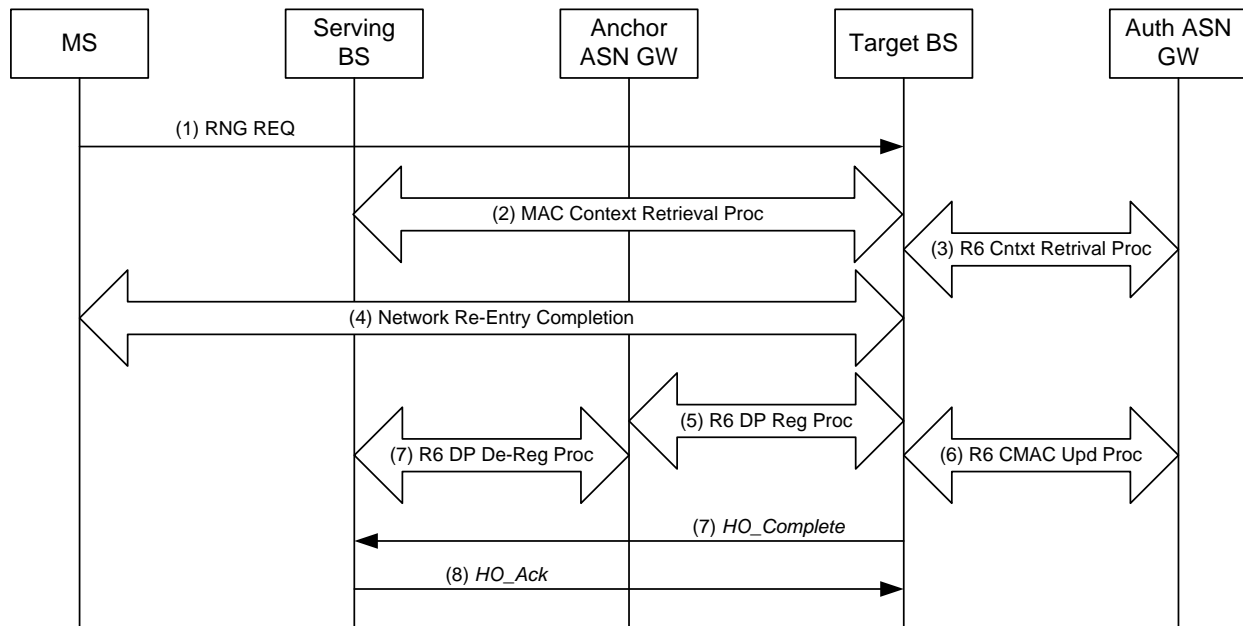
9       An Uncontrolled (Unpredictive) handover occurs when an MS starts ranging at a Target BS that wasn't previously  
10      notified of an impending handover from an MS and didn't participate in the Handover Preparation Phase. This may  
11      occur due to suboptimal radio planning conditions or MS implementation (handover notification of the Serving BS  
12      by MS is optional).

13      If an MS starts ranging with a BS that doesn't have MS Context information including Authenticator GW and  
14      Anchor ASN GW identifiers, the RNG-REQ message from the MS cannot be authenticated. In a worst case scenario  
15      a full Network Re-Entry will be required which results in a large delay, because some authentication methods may  
16      take seconds to complete, especially if the Home AAA Server is located far away and the communication is slow.

17      However if the MS includes the Serving BS ID TLV in the RNG-REQ message, the handover can still be completed  
18      in a reasonable delay and the period of traffic unavailability can be greatly reduced. When an MS re-enters at a  
19      Target BS and supplies its Serving BS ID in the RNG-REQ message, the Target BS may retrieve the relevant MS  
20      Context from the Serving BS including the Authenticator GW ID and Anchor ASN GW ID. Thus it becomes  
21      possible for the Target BS to authenticate the RNG-REQ and perform data path registration with the Anchor ASN  
22      GW. This call flow scenario is described in Figure 4-104.

23      Network Re-Entry might be completed immediately after receiving the MS Context or after data path establishment  
24      (the former case is shown in the call flows). The former method requires a lower Ranging Response Timeout in the  
25      MS, however it also requires holding the uplink traffic until the data path is established. The latter method doesn't  
26      require traffic holding but relies on larger Ranging Response Timeout in the MS. The moment of Network Re-Entry  
27      completion does not affect interoperability and is left as a vendor implementation option.

28      The following call flow provides an example of a successful uncontrolled handover scenario. A MS begins ranging  
29      at Target BS that wasn't contacted by the Serving BS to participate in the Handover Preparation phase. Therefore  
30      the Target BS was unaware of an impending arrival of the MS. The Target BS retrieves the MS context and  
31      authenticator information and successfully completes the handover.



**Figure 4-104 – Uncontrolled (Unpredictive) HO**

### STEP 1

An MS performs an uncontrolled handover by sending an RNG-REQ message to perform contention based ranging at a Target BS that didn't receive prior notification of an impending handover from the MS and therefore didn't participate in the Handover Preparation phase. The MS includes the Serving BSID 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 ASN GW ID and Anchor ASN GW ID.

### STEP 3

The Target BS requests AK context and service authorization info 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 Data Path ASN. 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-Data Path De-Registration procedure with the Serving BS.

**STEP 8**

Upon completion of network re-entry, the Target BS SHALL send a *HO\_Complete* message to notify the completion of the handover. Upon receipt of the *HO\_Complete* message, the Serving BS releases the MS context and starts timer  $T_{R8-HO\ Comp}$  or  $T_{R6-HO\ Comp}$  respectively.

**STEP 9**

The Serving BS sends a *HO\_Ack* message to the Target BS. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R8-HO\ Comp}$  or  $T_{R6-HO\ Comp}$  respectively.

**4.7.6.3 Message Definitions**

The composition of the messages over R6 and R8 in the context of HO is identical to the composition of the corresponding R4 messages described in section 4.8 except that only one target BS ID SHALL be included in the messages sent over R6 or R8.

**4.7.7 Data Integrity**

**4.7.7.1 Introduction**

Data Integrity refers to an optional set of procedures that may be applied during handover in order to minimize data loss. Data Integrity is not supported for uncontrolled HO cases.

The procedures explained here are applicable for Type 1 Data Path. Type 2 Data Path has inherent ARQ State anchoring mechanism that provides the same functionality in a different way.

Since each Service Flow may belong to different service class and may have different QoS requirements, Data Integrity may be required only for specific Service Classes. Whether Data Integrity method is to be applied to a service flow should be decided based on the SF QoS requirement information, SFA local policy information, and resource availability information of involved network entities.

Further negotiations SHALL be needed during handover time to choose the specific Data Integrity methods. Those negotiations may result in no Data Integrity procedures applied for a handover, if no agreement has been reached among involved functional entities.

During a handover, the Serving BS, Target BS and related network entities will report its Data Integrity Capability Information through existing handover and data path related control messages to Anchor ASN-GW.

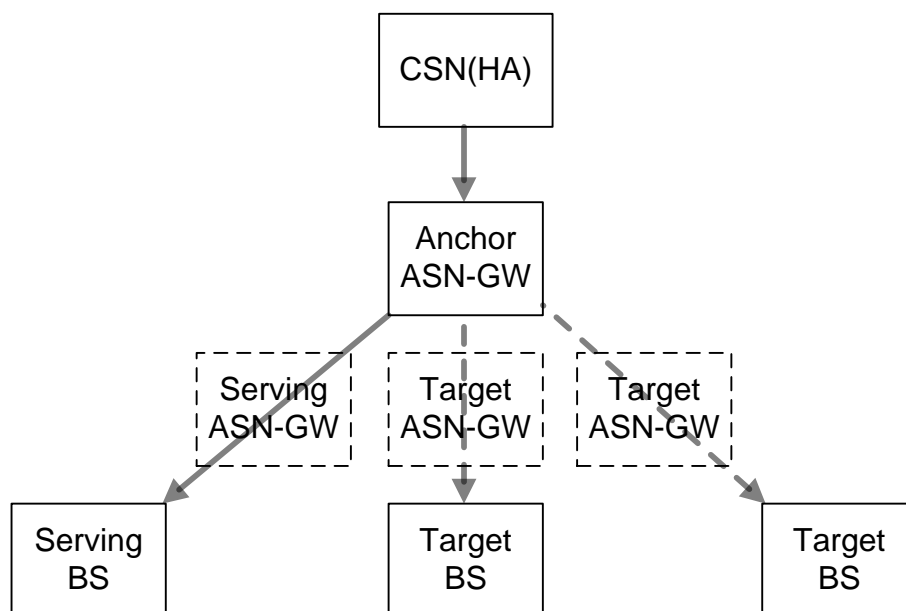
Since the Data Integrity functionality is essentially optional, special care has been taken to define negotiation of the Data Integrity Method to be applied. A particular Data Integrity Method can be selected only if all the involved network entities agree on it. Otherwise no Data Integrity method will be applied.

**4.7.7.2 Data Paths during handover**

Before handover, Data Path(s) exists only between the Anchor and the Serving BS (solid line in the Figure 4-105). On downlink, the Anchor ASN-GW classifies traffic incoming from R3 reference point and maps the classified IP packets onto per-Service-Flow GRE tunnels. Each GRE tunnel SHALL be identified by a GRE Key. For Service Flows that require Data Integrity, the Anchor ASN-GW SHALL also assign a GRE Sequence Number to each IP Datagram encapsulated in the GRE packet. The GRE Sequence Number SHALL be incremented by one with each new encapsulated IP Datagram per GRE Key (Service Flow).

If, during handover Preparation Phase, the Data Paths between the Anchor ASN-GW and each of the Target BSs are pre-established then the resulting Data Paths will take the form of a tree as it appears in Figure 4-105.





**Figure 4-105 – Per SF Data Path Tree after HO Preparation Phase**

Different GRE Keys may represent the same Service Flow on different branches of the Data Path Tree. If data are forwarded along the branches of the tree during HO, then the sequence numbers given to GRE packets to deliver the same IP datagrams SHALL be the same. The data may also be buffered at the Anchor ASN-GW or the Serving BS for later delivery on demand, to Target BS.

#### **4.7.7.3 Data Integrity without ARQ Synchronization**

This section explains Data Integrity operations without ARQ State Synchronization. If ARQ State synchronization is not supported between Serving BS and Target BS, the ARQ State Machine (for ARQ enabled Service Flows) at MS and Target BS SHALL be automatically reset after handover without any explicit ARQ reset notification. The MS SHALL be notified about the need to reset the ARQ State Machine by resetting the “Full Service and Operational State Transfer” bit in the “HO Process Optimization” bitmask that is delivered to the MS over the air. The Target BS transmits “HO Process Optimization” bitmask in RNG-RSP. The Serving BS transmits ‘HO Process Optimization’ bitmask in MOB\_BSHO-RSP or MOB\_BSHO-REQ. More details are available [13] section 6.3.21.2.8.1.6.3 “Service flows—dynamic context, ARQ enabled connections”.

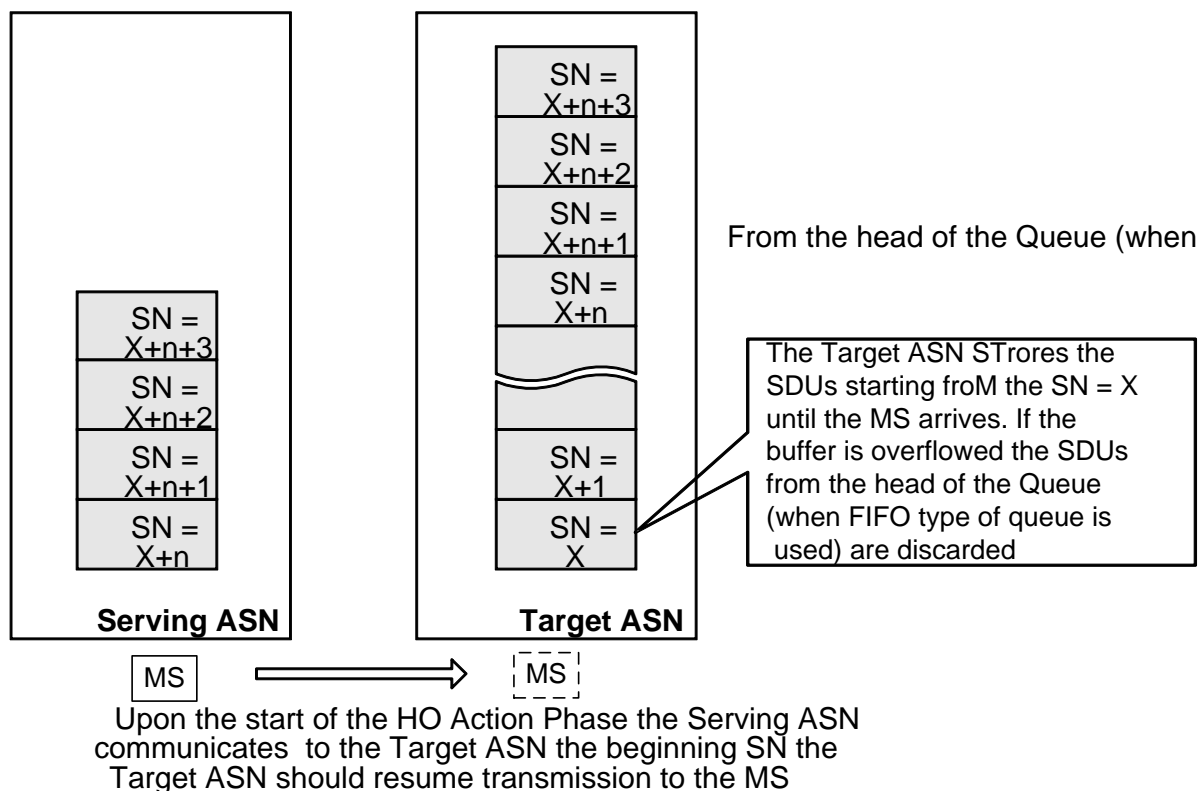
Data Integrity without ARQ Synchronization is applicable for both ARQ-enabled and ARQ-disabled Service Flows.

#### **4.7.7.3.1 Downlink Data Integrity Methods**

This section describes each specific method that can be applied for downlink data integrity support during handover.

##### **4.7.7.3.1.1 Multi-Unicasting Data Integrity Method**

Per-SF Selective Multi-Unicasting means that the data associated with the corresponding Service Flow is multi-unicast from the root of the Data Path tree (the Anchor ASN-GW) along the branches of the Data Path Tree to the entire set of the Target BSs. The data streams along each branch of the Data Path tree are replications of the stream flowing from the Anchor ASN-GW to the Serving BS which have same GRE Sequence Number. The SN of the first multi-unicast SDU is reported in the Pre-Registration Response. The SN of SDU to be used by the transmit buffer SHALL be the lower two byte of GRE Sequence Number of the received packet.



**Figure 4-106 – Transmission Queues in Serving BS and Target BS**

**Case: Data Path Setup from Target BS:** The Anchor ASN-GW starts multi-unicasting along the branches of the Data Path Tree immediately after Path Pre-Registration procedure has been finished. The SN of the first multi-unicast SDU that will be multi-unicasted toward this target is reported in the Path Pre-Reg\_Rsp message. Since Pre-Registration Requests from different Target BSs arrive to the Anchor ASN-GWs at different times the SN from which data delivery has started might be different for each branch of the Data Path Tree. The Target BS reports this SN to the Serving BS, so the latter knows which part of data is available in each Target BS. The Serving BS may then use this knowledge in order to deliver the data that are not yet available in the Target BSs to the MS prior to confirming handover with MOB\_BSHO-RSP or initiating handover with MOB\_BSHO-REQ.

**Case: Data Path setup from Serving/Anchor ASN-GW:** The Anchor ASN-GW starts multi-unicasting along the branches of the Data Path Tree along with Data Path Pre-Registration Request. The SN of the first multi-unicast SDU is reported in the Pre-Registration Request. The Target BS reports the SN to the Serving BS, so the latter knows which part of data is available in each Target BS. The Serving BS may then use this knowledge in order to deliver the data that are not yet available in the Target BSs.

Delivering the SN of the first multi-unicast SDU from the Target BS to the Serving BS is optional and may be omitted.

**SDU Transfer:** The Target BSs store the data until either the MS arrives or the handover is cancelled. The Figure 4-106 shows an example where multi-unicasting for a particular Service Flow started from the SDU with SN = X. Thus each Target BS stores SDUs starting from SN = X. If the storage buffer is overflowed the SDUs at the head of the Transmission Queue (i.e., older packets with lower SNs) may be discarded. If the buffer is overflowed in the Serving BS, it may discard the SDUs from the head of the Queue.

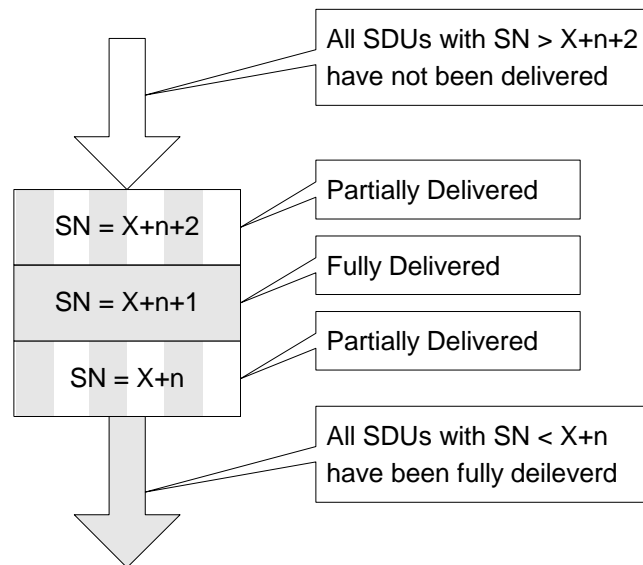
Meanwhile the Serving BS keeps transmitting the data to the MS. In Figure 4-106 it has transmitted n SDUs and the SDU with SN = X+n is at the head of the Transmission Queue. If the MS sends MOB\_HO-IND at this moment, the Serving BS will report to the Target BS (in the HO\_Cnf message) the last SDU SN that has not been transmitted (and acknowledged, for ARQ enabled connections) yet (i.e. SN = X+n on the Figure 4-106. Note that if ARQ is not supported, the serving ASN SHALL assume that the SDU with SN=X+n was successfully received by the MS. If

MOB\_HO-IND has never been received in the Serving BS and thus HO Confirm message has never been sent then the Target BS may retrieve the same information using Context Delivery Transaction.

Thus the Target BS will know that it needs to resume transmission from the SDU with SN =  $X+n$  and should discard all the SDUs with lower SNs. The other way is to let MS send SDU SN Feedback Header with the last SDU SN (SN =  $X+n$ ) on the uplink channel to the Target ASN as described in 4.7.7.3.3.

If ARQ is enabled certain SDUs may have some ARQ blocks acknowledged and some may not. SDUs that have some ARQ blocks unacknowledged are treated as untransmitted yet (i.e. all the blocks will be transmitted anew in the Target BS).

It may happen that the Transmission Queue in the Serving BS consists of partially delivered (partially acknowledged) SDUs interleaved with fully delivered SDUs. For example the Serving BS could receive acknowledgements for all the blocks of the SDU with SN =  $X+n+1$  while only part of blocks of the SDU with SN =  $X+n$  and the SDU with SN =  $X+n+2$  were acknowledged. Figure 4-107 illustrates the example.



**Figure 4-107 – Example of Transmission Queue in the Serving BS**

In this case the Serving BS should report to the Target BS the list of the SNs of the SDUs that have to be transmitted anew – in this example the list would include  $\{X+n, X+n+2\}$ . All the SDUs with the SNs lower than the lowest SN (i.e. SNs  $< X+n$ ) in the list have been successfully delivered to the MS. Since the SDU with SN =  $X+n+1$  has already been fully delivered, it will not be transmitted anew from the Target BS. All the SDUs with SNs higher than the highest SN in the list have not been transmitted yet. The Target ASN should re-transmit the SDUs specified in the list and then resume transmission from the SDU with the SN that is next after the SDU with the highest SN in the list.

If ARQ is enabled, the MS should reset ARQ parameters after Re-Entry in the Target BS. This ARQ parameter reset will happen automatically after HO completion at the Target BS.

#### 4.7.7.3.1.2 Buffering with Delivery on Demand Data Integrity Method

Per-SF Selective multi-unicasting explained in 4.7.7.3.1.1 provides for immediate availability of data in the Target BS at the moment of completion of handover. However it also poses additional capacity requirements on the backhaul network between the Anchor ASN-GW and the Target BS/ASN-GWs.

Note also, that the Multi-Unicasting Data Integrity method implies buffering requirements at the Target BS(s). If additional backhaul capacity or buffer resources are not available at the Target BS(s), the buffering might be delegated to the Anchor ASN-GW. In this case the Anchor ASN-GW, instead of sending the replicated data along the branches of the Data Path Tree, buffers the data until their delivery is explicitly requested via a Path Registration Request message from one of the Target BSs (TBSs).

Buffering in Anchor ASN-GW follows the same rules as buffering in Target BS described in Sec. 4.7.7.3.1.1.

The Anchor ASN GW starts buffering immediately after receiving a Pre-Registration Request from any one of the Target BSs. Anchor ASN-GW maintains a single buffer for all Data Path Trees.

The SN of the first buffered SDU is reported in the Path\_Pre-Reg Rsp message for target initiated path pre-registration procedure or Path Pre-Reg Req message for Serving/Anchor initiated path pre-registration procedure. The Target BS, in turn, reports the SN to the Serving BS with HO Response, so the Serving BS knows from which part of data can be delivered to Target BS on demand. The Serving BS may then use this knowledge in order to deliver to MS the data that are not available in the Target.

The Serving BS delivers to the Target BS the information about the SDUs it has successfully delivered and about the SDUs that need to be delivered by the Target BS. The information is delivered with either HO Confirm message or Context Delivery Transaction in the way identical to that explained in Sec. 4.7.7.3.1.

#### **4.7.7.3.1.3 BS Buffer Switching Method**

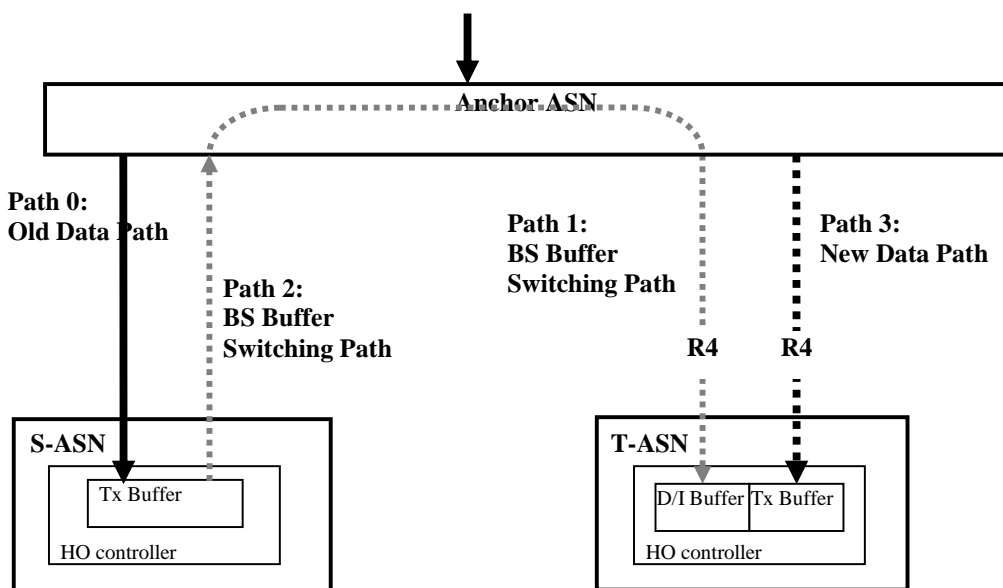
This data integrity method requires data buffering at the Serving BS and forwarding the buffered data to the selected Target BS(s) during the HO action phase.

At the start of HO Action phase, all downlink data packets that are sent by the Anchor ASN-GW SHALL be buffered at the Serving BS and, at the same time, optionally at the Target BS. Data packets buffered at the Serving BS SHALL be forwarded to the selected Target BS during the HO Action phase. The data buffering function SHALL be co-located with the handover decision making entity within the BS.

The data SHALL be forwarded to the Target BS(s) in one of two ways:

- Via the Anchor ASN-GW, through R6/R4 data paths. For more details, refer to section 4.7 for R6/R4 handoff procedure.
- OR
- Via the R8 data paths that have been setup between the BSs, if the optional R8 data path establishment procedure for data integrity is supported

#### 4.7.7.3.1.3.1 Data Delivery via Anchor ASN-GW



\* Note: Dual buffers are shown at the Target BS for illustration purpose only.

**Figure 4-108 – Data buffering and forwarding in BS Buffer Switching**

##### 4.7.7.3.1.3.1.1 Operations during HO Preparation phase

For this method, the ASN-GW SHALL forward data packets to the Serving BS as it does before the handover and the Serving BS SHALL transmit packets to MS via 802.16e air interface.

The Target BS(s) MAY initiate the pre-registration of Buffer Switching path - path 1 in the figure (in the downlink direction) - with the Anchor ASN-GW, before sending a HO Response to the Serving BS. Completion of Buffer Switching path(s) between the Anchor and the Target BS(s) SHALL trigger the Anchor ASN-GW to start pre-registration of Buffer Switching path between the Anchor ASN-GW and the Serving BS - path 2 in the figure (in the uplink direction). Data delivery trigger TLV within the path pre-registration message for setup of buffer switching paths SHALL be set to zero. Buffer switching path enables the Serving BS to forward the data traffic to the Target BS(s) via Anchor ASN-GW.

##### 4.7.7.3.1.3.1.2 Operations during Action Phase

In the HO Action phase, upon receiving MOB\_HO-IND message from the MS, the Serving BS SHALL stop transmitting packets for MS via the 802.16e air interface.

If the handover data integrity feature is supported per the BS buffer switching method, the Serving BS SHALL deliver the transmission status information of its buffered packets to the Target BS in a HO\_Cnf message. The message SHALL include the SDU SN of the first SDU to be sent to the MS by the Target BS.

After receiving the HO\_Cnf message, if the BS Buffer Switching paths (data paths 1, and 2 in the Figure 4-108) and New Data Path (data path 3 in the Figure 4-108) are not pre-registered, the Target BS SHALL initiate the Path Registration procedure to set up a Buffer Switching path (path 1) between the Anchor and the Target BS, in addition to the Path Pre-Registration procedure to setup a data path(s) which SHALL replace, after the handover, the previous R4 data path(s) between the Serving BS and the Anchor ASN GW (path 0). After establishing a Buffer Switching path between the Target and the Anchor ASN-GW, the Anchor ASN-GW SHALL send a Path\_Reg\_Req message to the Serving BS to initiate a path registration procedure for a Buffer Switching path between the Serving and the Anchor ASN-GW (path 2). If the Buffer Switching path(s) has already been established during the HO Preparation phase, then this path registration procedure SHALL be skipped in the HO Action phase.

1 Upon completion of the Buffer Switching path(s) between the Serving BS and the Anchor ASN-GW, the Serving  
2 BS SHALL start forwarding data packets which have been buffered at the Serving BS for air transmission at the  
3 Target BS.

4 If the Serving BS can determine that the MOB\_HO-IND is lost in the air or receives MOB\_HO-IND without BS ID,  
5 then the Serving BS MAY send \_HO-Cnf with Unconfirmed indicator and forward buffered data packets to all  
6 candidates Target BS(s) which were indicated in the MOB\_BSHO\_RSP or MOB\_BSHO\_REQ.

7 If R4 data path(s) between the Anchor and the Target BS is pre-registered during the action phase, Target BS(s)  
8 MAY choose to activate the data transfer immediately. Hence, Anchor ASN-GW MAY start bi-casting of data  
9 packets (which are received by the Anchor ASN-GW via the R3 reference point) towards both the Serving and the  
10 Target BS. By default, Anchor ASN-GW SHALL send data packets towards the Serving BS.

#### 11 **4.7.7.3.1.3.1.3 Operations during Network re-entry.**

12 Upon successful re-entry of MS at the Target BS, the Target ASN-GW SHALL send Path\_Reg\_Req message, which  
13 requests setup of New Data path (data path 3 in the Figure 4-108), and notifies the Anchor ASN-GW of the  
14 successful re-entry.

15 After receiving Path\_Reg\_Req from the Target BS, the Anchor ASN-GW SHALL stop forwarding data packets  
16 towards the Serving BS and switch data transmission to the Target BS. The SDU SN of the last transmitted data  
17 packet to the Serving BS SHALL be transmitted to the Target BS during the path registration between the Anchor  
18 and the Target BS (in Path Reg resp from Anchor ASN-GW). Timer  $T_{Wait\_ServingBS\_SendEnd}$  is started After Target BS  
19 receives Path Reg RSP. After  $T_{Wait\_ServingBS\_SendEnd}$  is expired, the Target BS starts sending packets in the  
20 New Data buffer. Successful completion of the Path Registration procedure between the Anchor ASN-GW and the  
21 Target BS causes the Anchor ASN-GW to initiate the Data Path De-Registration procedure with the Serving ASN to  
22 remove the original data path (Path 0 in the figure). The SDU SN(sn) for the last transmitted packet by the Anchor  
23 ASN-GW is forwarded to the Serving BS in the data path deregistration request message so that the Serving BS can  
24 ensure that all the data packets are received before responding to the data de-registration request message from the  
25 anchor. The Target BS starts buffering the data received from Anchor ASN-GW in Tx Buffer.

26 The SDU SN for the packet, last transmitted by the Anchor ASN-GW, can be forwarded to the Target BS in the data  
27 path registration response message. Target BS SHALL use this sequence number(sn) as well as the sequence  
28 number of the next packet destined for MS received in the HO Confirm message(sn') to ensure that all the data  
29 packets are received before the data path deregistration procedure for the Buffer Switching path(s). Upon receipt of  
30 the last packet, the-Target BS initiates the data path deregistration procedure for the Buffer Switching path(s) with  
31 the Anchor ASN for the buffer switching path(s). This automatically triggers the Anchor ASN-GW to initiate  
32 deregistration of the BS Buffer Switching path(s) with the Serving BS.

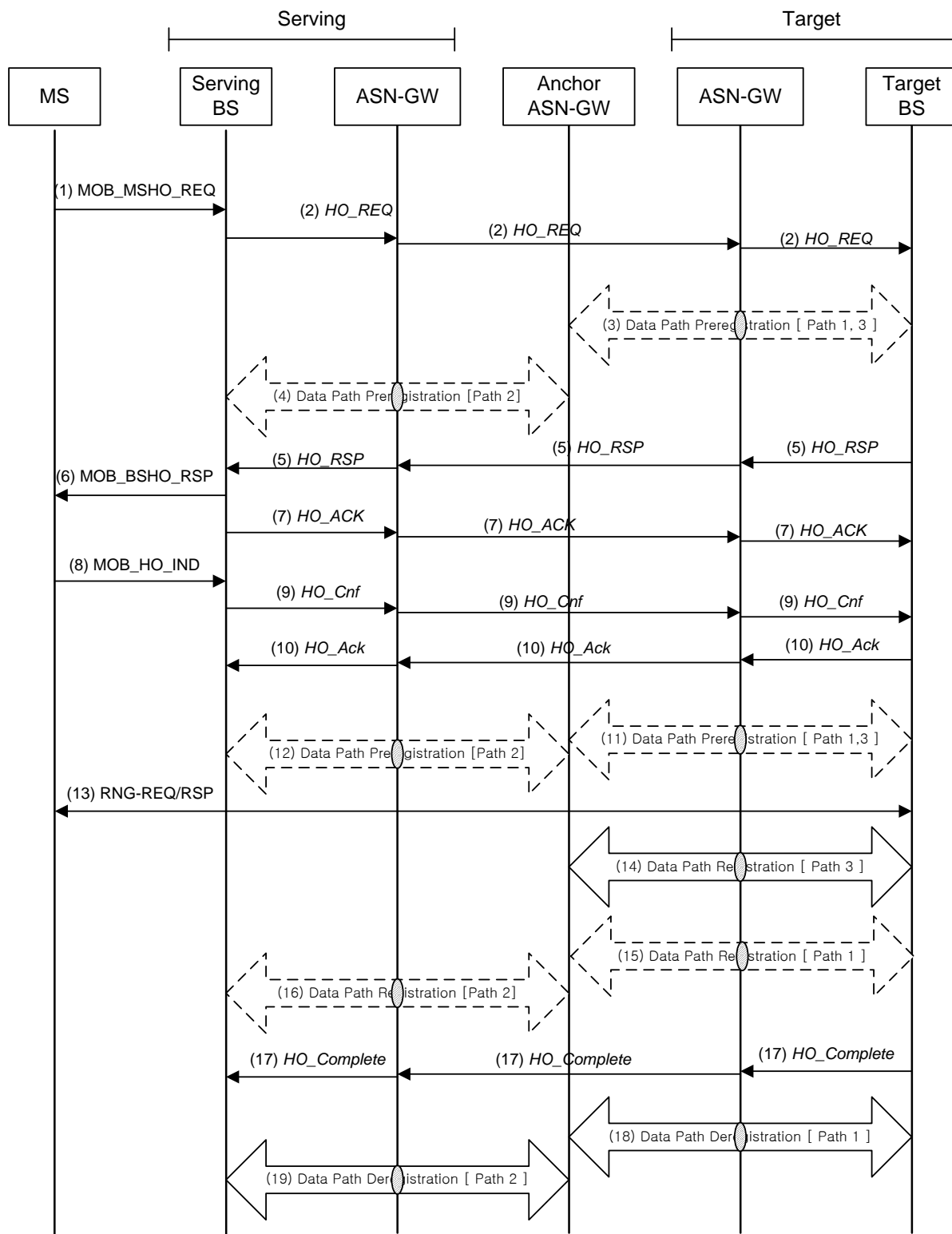
33 This step is important to ensure no data packets are lost during the data path de-registration procedure. In the Target  
34 BS, there will be no overlapping of packets between D/I buffer and Tx buffer.

35 If optional bi-casting procedure was performed during the action phase, the Target BS performs sequence number  
36 management to synchronize the buffers. If the Target BS receives a packet, through the BS Buffer Switching path,  
37 whose sequence number is equal to or greater than the sequence number of the head-of-line packet in the Tx buffer,  
38 the Target BS SHALL trigger the Data Path De-registration procedure with the Anchor ASN-GW to remove the  
39 Buffer Switching path between the Anchor and the Target BS, which in turn causes the Anchor ASN-GW to initiate  
40 the data path de-registration of the Buffer Switching path between the Anchor ASN-GW and the Serving BS.

41 The Serving BS SHALL NOT flush its buffer until the data path de-registration procedure for the buffer switching  
42 path has been initiated. Upon receiving HO Complete message, Serving BS SHALL ensure that all the packets have  
43 been transferred to the Target BS prior to releasing the MAC context and data path(s).

44 The Target BS SHALL resume data transmission to MS by sending data packets received from the Serving BS first.  
45 In the Target BS, the data that was received from the Serving BS (D/I buffer) is transmitted to the MS sequentially  
46 prior to transmitting the data received from the Anchor ASN-GW (Tx buffer) to maintain data integrity and ordered  
47 delivery of packets to MS. After successful transmission of packets buffered in the D/I buffer, the target BS SHALL  
48 flush the buffer.

1 **4.7.7.3.1.3.1.4 Handover Call Flows**



**Figure 4-109 – Data Delivery via Anchor ASN-GW**

**STEP 1**

The MS initiates a handover by sending a MOB\_MSHO-REQ message to the serving BS which includes one or more potential target BS's.

**STEP 2**

The serving BS sends an *HO\_Req* message to one or more potential target BS's selected for the handover and starts timer  $T_{R6\_HO\_Request}$  for each message. Relay ASN-GW relays the *HO\_Req* message.

**STEP 3**

Optional: The target BS initiates pre-establishment of a data path from the Anchor ASN-GW to its data integrity buffer (path 1) and a data path from the Anchor ASN-GW to its transmit buffer (path 3) by invoking the Data Path Pre-Registration procedure (see section 4.12.1).

**STEP 4**

Optional: Upon receipt of the data path pre-registration request from the target BS to its data integrity buffer (path 1), the Anchor ASN-GW initiates a data path from the Serving BS to the Anchor ASN-GW (path 2) to complete a buffer switching path from the serving BS to the target BS by invoking the Data Path Pre-Registration procedure (see section 4.12.1). The *data delivery trigger* TLV in the path pre-registration request message is set to 0. The serving BS begins buffering data packets received from the anchor ASN-GW.

**STEP 5**

The target BS(s) sends a *HO\_Rsp* message to the serving BS to acknowledge the handover request and starts  $T_{R6\_HO\_Rsp}$ . Upon receipt of the *HO\_Rsp* message, the serving BS stops timer  $T_{R6\_HO\_Req}$ .

**STEP 6**

The Serving BS sends a MOB\_BSHO-RSP message to the MS.

**STEP 7**

The serving BS sends a *HO\_Ack* message to the target BS(s). Upon receipt of the *HO\_Ack* message, the Target BS(s) stops timer  $T_{R6\_HO\_Rsp}$ .

**STEP 8**

The MS sends a MOB\_HO-IND message to the serving BS to notify it of its intent to handover to a target BS as proposed by the serving BS in the handover preparation phase.

**STEP 9**

Upon reception of the MOB\_HO-IND message, the Serving BS sends a *HO\_Cnf* message to the Target BS and starts timer  $T_{R6\_HO\_Conf}$ .

**STEP 10**

The Target BS sends a *HO\_Ack* message to the Serving BS. Upon receipt of the *HO\_Ack* message, the Serving BS stops timer  $T_{R6\_HO\_Conf}$ . If data path pre-registration occurred in steps 3 and 4, the serving BS begins transferring data packets to the target BS via the Anchor ASN-GW (path 2 and path 1) starting with the first packet to be transmitted to the MS. The target BS buffers the packets in its data integrity buffer.

**STEP 11**

If data path pre-registration was not optionally performed in step 3, the target BS initiates pre-establishment of a data path between from the Anchor ASN-GW to its data integrity buffer (path 1) and a data path from the anchor ASN-GW to its transmission buffer (path 3) by invoking the Data Path Pre-Registration procedure (see section 4.12.1).



**STEP 12**

If not optionally performed in step 4, upon receipt of the data path pre-registration request from the target BS for a data path from the anchor ASN-GW and the target BS's data integrity buffer (path 1), the anchor ASN-GW initiates registration of a data path from the serving BS to the anchor ASN-GW (path 2) to complete a buffer switching path from the serving BS to the target BS (see section 4.12.1). The *data delivery trigger* TLV in the path pre-registration request message is set to 1. The serving BS begins transferring data packets received from the anchor ASN-GW to the target BS via the anchor ASN-GW (path 2 and path 1) starting with the first packet to be transmitted to the MS. The target BS buffers the packets in its data integrity buffer.

**STEP 13**

The MS initiates network re-entry at the Target BS. The target BS begins transmitting data packets to the MS starting with data packets buffered in its data integrity buffer.

**STEP 14**

The Anchor ASN-GW and Target BS perform data path registration procedure for path 3.

**STEP 15**

If data path pre-registration did not optionally occur in steps 3 or 11, the target BS initiates a data path from the Anchor ASN-GW to its data integrity buffer (path 1) by invoking the data Path Registration procedure.

**STEP 16**

If data path pre-registration did not optionally occur in steps 4 or 12, upon receipt of the data path pre-registration request from the target BS for a data path from the anchor ASN-GW and the target BS's data integrity buffer (path 1), the anchor ASN-GW initiates registration of a data path from the serving BS to the anchor ASN-GW (path 2) to complete a buffer switching path from the serving BS to the target BS (see section 4.12.1). The *data delivery trigger* TLV in the path pre-registration request message is set to 1. The serving BS begins transferring data packets received from the anchor ASN-GW to the target BS via the anchor ASN-GW (path 2 and path 1) starting with the first packet to be transmitted to the MS. The target BS buffers the packets in its data integrity buffer.

**STEP 17**

The target BS sends a *HO\_Complete* message to notify the serving BS that the MS was successfully acquired. Upon receipt of the *HO\_Complete* message, the serving BS releases the MS context and starts timer  $T_{R6\_HO\_Comp}$ .

**STEP 18**

The target BS initiates deregistration of the data path between its data integrity buffer and the anchor ASN-GW (path 1) upon completing reception of buffered packets for the MS by invoking the Data Path De-Registration procedure (see section 4.13).

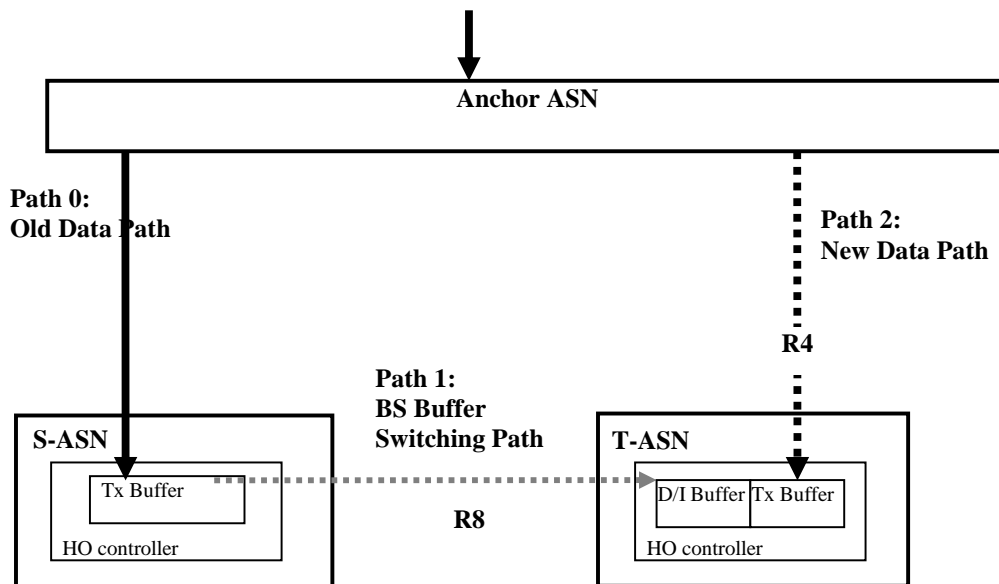
**STEP 19**

Upon receipt of a request to deregister the data path between the anchor ASN-GW and the target BS's data integrity buffer (path 1), the anchor ASN-GW initiates the deregistration of the data path between the anchor ASN-GW and the serving BS (path 2) by invoking the Data Path De-Registration procedure (see section 4.13).

Note: Serving BS may initiate de-registration of data path 0 at any time after step 16 and/or expiration of the resource retain timer.

#### 4.7.7.3.1.3.2 Direct Data Delivery Method

In this method the buffered data is delivered to the Target BS directly using R8 data path between the BSs.

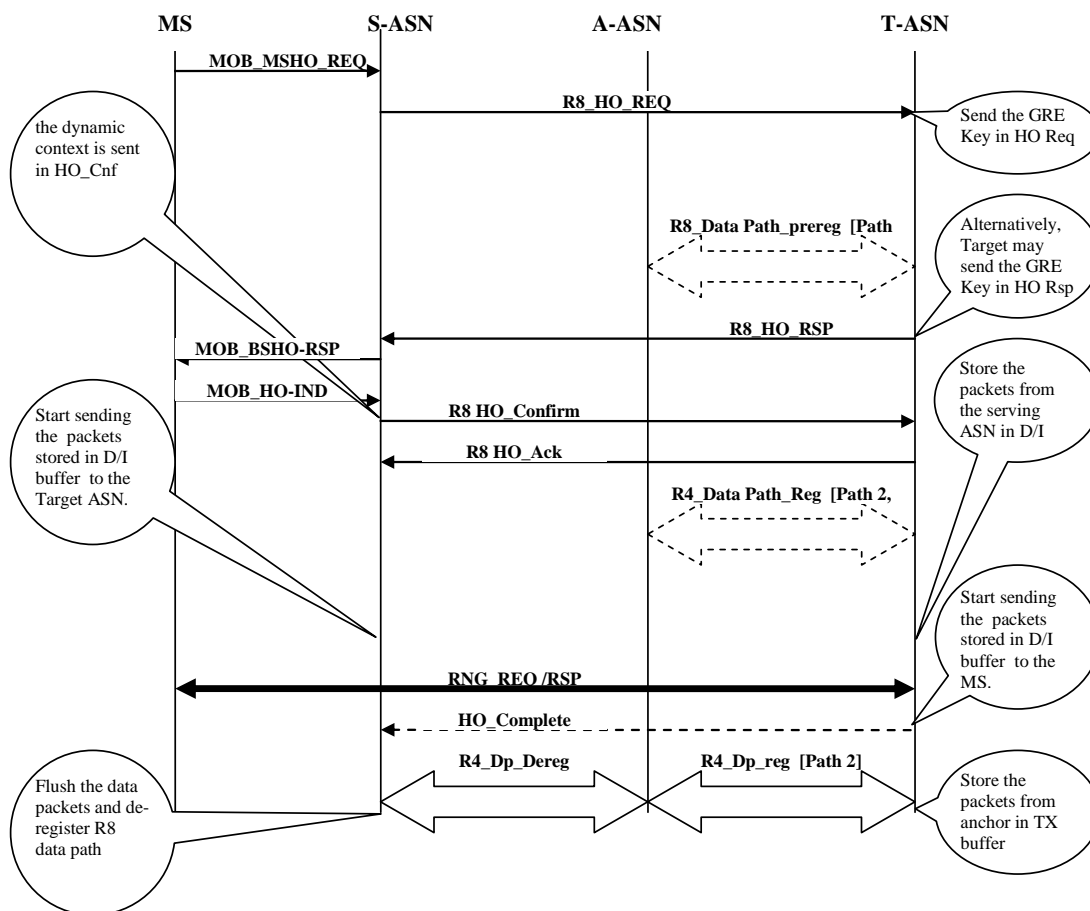


**Figure 4-110 – Data buffering at the Serving BS and forwarding via R8**

\*Note: Reference to D/I buffer here is for illustration purpose.

#### 4.7.7.3.1.3.2.1 Operations during Preparation Phase

The Target BS(s) MAY pre-register data paths (Path 2) with the Anchor ASN-GW after receiving the HO-REQ. Data delivery trigger SHALL be turned off in the data path pre registration procedure between the Target BS(s) and the Anchor ASN-GW to avoid multi uni-casting to the target. Capability negotiation for R8 data path setup between Serving BS and Target BS is shown in section 4.7.7.5. For the purpose of setting a direct data path (path 1) between the Serving BS and the Target BS, GRE Keys for R8 data path may be exchanged between the Target BS and the Serving BS via R8 HO Request / HO response without sending an explicit path registration message. Data Delivery trigger TLV within the path prereg message used for setting up the buffer switching path SHALL be set to 0. Different GRE keys represent the same service flow on different branches of the data path tree if the data is forwarded to multiple ASNs.



**Figure 4-111 – Data integrity procedures for Direct data delivery method**

#### 4.7.7.3.1.3.2.2 Operations during Action Phase

Upon receipt of MOB\_HO-IND message with the selected Target BS ID from the MS, the Serving BS sends HO confirm to the Target BS. If the data path between the Target BS and the Anchor ASN-GW is not already established, the Target BS SHALL pre-register new data path (path 2). Similarly, if the direct data path (BS buffer switching path) to the Serving BS is not already established, Target BS SHALL register an R8 data path at this time. HO confirm message MAY be used as a trigger for the data forwarding from the Serving BS over the R8 data path between the Serving and Target BS. The SDU SN of the next packet destined for MS is forwarded to the Target BS in the HO Confirm message initiated by the Serving BS. Upon activation of data path, Serving BS initiates the data transfer to the Target BS via the GRE tunnel or it may choose to buffer the packets. This is based on the local policies. Target BS buffers these packets received over R8 in D/I buffer.

Optionally, if the Serving BS determines upon expiry of the scheduled timer (refer to 16e for more details) that the MOB\_HO-IND was lost in the air or receives MOB\_HO-IND without BS ID, the Serving BS sends HO confirm with un-confirm indication and may initiate data transfer to all candidate Target BS(s) which were indicated in the MOB\_BSHO-RSP or MOB\_BSHO-REQ.

Optionally, if data path(s) (Path 2) between the Anchor ASN-GW and the Target BS is pre-registered during the action phase, the Target BS(s) MAY choose to activate the data transfer immediately. Hence, Anchor ASN-GW MAY start bi-casting data packets (which are received by the Anchor ASN-GW via the R3 reference point) towards both the Serving and the Target BS(s).

#### 4.7.7.3.1.3.2.3 Operations during Network Entry Phase

Upon successful completion of network re-entry of the MS, Target BS SHALL send Data path registration request message to set up a new Data Path and notify the Anchor ASN-GW of the successful re-entry of MS, and starts forwarding the data packets from D/I buffer to the MS. In parallel, Target BS also initiates data path registration procedure to the Anchor ASN-GW. Anchor ASN-GW switches downlink traffic from the Serving BS to the Target BS and initiates data path deregistration procedure to the Serving BS. The SDU SN(sn) for the last transmitted packet by the Anchor ASN-GW is forwarded to the Serving BS in the data path deregistration request message so that the Serving BS can ensure that all the data packets are received before responding to the data de-registration request message from the Anchor ASN-GW. This step is important to ensure no data packets are lost during the data path de-registration procedure. Meantime, the Target BS starts buffering the data received from Anchor ASN-GW in Tx Buffer.

The Serving BS completes the transfer of all the data in its resource retention buffer to the Target BS. If HO complete is received, Serving BS SHALL ensure that all the packets have been transferred to the Target BS prior to releasing the MAC context.

For ARQ enabled Service flows, the SDUs with Block Sequence Numbers (BSNs) which are not acknowledged are also sent to the Target BS.

The SDU SN (sn) for the last transmitted packet by the Anchor ASN-GW can be forwarded to the Target BS in the data path registration response message. Target BS SHALL use this sequence number(SN) as well as the sequence number of the first unsent packet destined for the MS received in the HO Confirm message to ensure that all the data packets are received before initiating the R8 data de-registration request message to the Serving BS. Upon receipt of the last packet, the-Target BS initiates the data path deregistration procedure for the Buffer Switching path(s) with the Serving BS.

This step is important to ensure no data packets are lost during the data path de-registration procedure. In the Target BS, there will be no overlapping of packets between D/I buffer and Tx buffer.

If optional bi-casting procedure was performed during the action phase, the Target BS performs sequence number management to synchronize the buffers. If the target receives a packet, through the BS Buffer Switching path, whose sequence number is equal to or greater than the sequence number of the head-of-line packet in the Tx buffer, the Target BS SHALL ensure the Data Path De-registration procedure with the Serving BS to remove the Buffer Switching path between the Serving and the Target BS, which in turn causes the Anchor ASN-GW to initiate the data path de-registration of the old data path between the Anchor ASN-GW and the Serving BS.

The Serving BS SHALL not flush its buffer until the data path de-registration procedure for the buffer switching path has been initiated. If HO complete is received, Serving BS SHALL ensure that all the packets have been transferred to the Target BS prior to releasing the MAC context and data path(s).

In the Target BS, the data that was received from the Serving BS (D/I Buffer) is transmitted to the MS sequentially prior to transmitting the data received from the Anchor ASN-GW (Tx Buffer) to maintain data integrity and ordered delivery of packets to MS.

[Note]: Refer to Stage3 ASN Anchored Mobility section for details of releasing MAC context.

#### 4.7.7.3.2 Uplink Data Integrity

Uplink Data Integrity support is required when ARQ synchronization is supported. It is only required that the Serving BS delivers to the Target BS the SN from which the Target BS should start numbering its uplink SDUs.

If the Serving BS has some uncompleted SDUs received from MS it SHALL discard them after De-Registration of Data Path with the Anchor ASN-GW.

#### 4.7.7.3.3 Auxiliary Use of SDU SN Report

The Serving and Target BSs and the MS may perform MS-Assisted coordination of DL transmission during handover as described in 802.16e section 6.3.22.2.8. The Target BS may signal to the MS on the intention to apply this procedure by using Bit #11 of 'HO Process Optimization' bitmask in the RNG-RSP message. The Serving BS may transmit 'HO Process Optimization' bitmask in the MOB\_BSHO-RSP or MOB\_BSHO-REQ messages.

For ARQ enabled connections, the MS may report to the Target BS the next ARQ BSN in the special header defined in 802.16e section 6.3.2.1.2.1.7. After reception of the header, the TBS SHALL resume transmission of the data of the corresponding DL Service Flow starting from the BSN specified in the header.

The report from MS takes precedence over the ARQ Sync information received from the Serving BS in case of mismatch.

For ARQ disabled connections, the MS may report to the Target BS the next SDU SN in the special header defined in 802.16e section 6.3.2.1.2.1.7. The coordination of the SDU SNs between the MS and the BS is described in 892.16e section 6.3.22.2.8. The Serving BS should make sure that SDU SN in the MS is equal to the remainder of integer division by 255 of the corresponding SDU SN in the GRE Header. The Target BS should make sure that SDU numbering in the MS continues after handover.

#### 4.7.7.3.4 Informational Elements Added by this Functionality

Only Informational Elements related to the operation of the Data Integrity without ARQ Synchronization are described in this section. The Informational Elements related to the negotiation of the Data Integrity method are described in 4.7.7.

The Table 4-104 shows how the SN of the first Multi-Unicast/Buffered SDU and Data Path information of BS Buffer Switching method are delivered in HO Request/Response messages.

**Table 4-104 –Info in HO\_Req**

<u>IE</u>	<u>Reference</u>	<u>M/O</u>	<u>Notes</u>
MS Info	5.3.2.103	M	
>SF Info (one or more)	5.3.2.185	M	
>>SFID	5.3.2.184	M	
>>SDU Info	5.3.2.176	O	Description of the first Multi-Unicast/Buffered SDU. Included for downlink SFs only.
>>>SDU SN	5.3.2.178	CM	SN of the first Multi-Unicast/Buffered SDU.  This TLV SHALL be included if SDU Info is included in the transmitted message.
>>Data Path Info	5.3.2.45	M	
>>>Data Path ID	5.3.2.44	CM	This TLV SHALL be included if Data Path Info is included in the transmitted message.

The Table 4-105 shows how the SN of the first Multi-Unicast/Buffered SDU and Data Path information of BS Buffer Switching method are delivered in Path Pre-Registration Request/Response messages.

**Table 4-105 – Switching Data Path ID & SDU Info in Path Pre-Reg\_Req/Rsp**

IE	Reference	M/O	Notes
Registration Type	5.3.2.145	M	Add one more option to indicate the path setup for BS buffer switching method.  Possible values include: 0: Initial Network Entry 1: Handover 2: In-Service Data Path Establishment 3: MS Network Exit 4: Idle Mode Entry and Idle Mode Exit
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.
>SF Info (one or more)	5.3.2.185	M	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	O	
>>>Data Path ID	5.3.2.44	CM	
>>>Switching Data Path ID	5.3.2.383	O	It SHALL be used when the Data Integrity method of BS buffer switching is selected. This indicates GRE Key for data path which SHALL be used to forward data packets buffered at the Serving BS.
>>SDU Info	5.3.2.176	O	Description of the first Multi-Unicast/Buffered SDU. Included for downlink SFs only.
>>>SDU SN	5.3.2.178	CM	SN of the first Multi-Unicast/Buffered SDU.  This TLV SHALL be included if SDU Info is included in the transmitted message.

The Table 4-106 specifies placement and meaning of the SDU Info in HO Confirm or Context Report from the Serving BS to the Target BS.

**Table 4-106 – SDU Info in HO\_Cnf or Context\_Rpt From Serving BS to Target BS**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.
>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	CM	SFID associated with the Service Flow.  This TLV SHALL be included if SF Info is included in the transmitted message.
>>SDU Info (one or more)	5.3.2.176	O	The list of SDUs in the transmission (for downlink) or reception (for uplink) queue in the Serving BS.  For downlink SFs the greatest SN is the SN of the SDU from which the transmission should be resumed. Prior to that the rest of the SDUs referred to in the list should be transmitted.  For uplink SFs the list indicates the SDUs the Target BS may expect to receive from the MS.
>>>SDU SN	5.3.2.178	CM	The SN for the last unsent SDU.  This TLV SHALL be included if SDU Info is included in the transmitted message.

**Table 4-107 – SDU SN in Path\_De-Reg Req from Serving ASN GW to Serving BS, Anchor ASN-GW to Serving BS**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.
>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	CM	SFID associated with the Service Flow
>>SDU Info (one or more)	5.3.2.176	O	The list of SDUs in the transmission (for downlink) or reception (for uplink) queue in the Serving ASN.  For downlink SFs the greatest SN is the SN of the SDU from which the transmission should be resumed. Prior to that the rest of the SDUs referred to in the list should be transmitted.  For uplink SFs the list indicates the SDUs the Target ASN may expect to receive from the MS.
>>>SDU SN	5.3.2.178	CM	The SN for the last transmitted SDU.

The exact formats of the TLVs that implement the discussed Informational Elements are specified in section 5.

#### 4.7.7.4 Data Integrity with ARQ Synchronization

Data Integrity procedures may involve ARQ State Synchronization between the Serving BS and Target BS. ARQ State Synchronization is optional and is negotiated between the Serving and Target BS. It is added on the top of related basic Data Integrity procedures specified in 4.7.7.3.

If ARQ State is synchronized between Serving BS and Target BS for ARQ enabled Service Flows the MS and the Target (New Serving) BS resume data transmission from the very point it stopped between the MS and Old Serving ASN when handover happened.

If ARQ State Synchronization is agreed between the Serving and Target BS, then the MS SHALL be notified of expected ARQ Synchronization by setting the “Full Service and Operational State Transfer” bit in the “HO Process Optimization” bitmask that is delivered to the MS over the air.

The Target BS transmits “HO Process Optimization” bitmask in RNG-RSP. The Serving BS (Serving BS) transmits ‘HO Process Optimization’ bitmask in MOB\_BSHO-RSP or MOB\_BSHO-REQ. More details are available *IEEE 802.16e section 6.3.22.2.8.6.3*.

Data Integrity with ARQ Synchronization is applicable for ARQ enabled Service Flows.

##### 4.7.7.4.1 Synchronization of ARQ State

###### 4.7.7.4.1.1 IEEE 802.16e ARQ State Machine

The Transmitter ARQ State Machine is described in *IEEE 802.16e standard, section 6.3.4.6.2*. The Receiver ARQ State Machine is described in *IEEE 802.16e standard, section 6.3.4.6.3*. The parameters of the State Machines are defined in *IEEE 802.16e, section 6.3.4.3*. The Table 4-108 lists these parameters.

**Table 4-108 –**

<u>Parameter</u>	<u>Description</u>
ARQ_BSN_MODULUS	Number of unique BSN values, i.e., $2^{11}$ . This is a constant value.  IEEE 802.16e MAC divides the SDUs onto logical parts called Blocks. All Blocks are of equal size except from the last one in the SDU (the Block Size is a per Connection parameter). Each Block is assigned a sequence number called Block Sequence Number – BSN. The IEEE 802.16e MAC ARQ works with BSNs.
ARQ_WINDOW_SIZE	The maximum number of unacknowledged ARQ blocks at any given time. An ARQ Block is unacknowledged if it has been transmitted but no acknowledgment has been received. The number SHALL be less than or equal to half of the ARQ_BSN_MODULUS.
ARQ_BLOCK_LIFETIME	The maximum time interval an ARQ block SHALL be managed by the transmitter ARQ state machine, once initial transmission of the Block has occurred. If transmission (or subsequent retransmission) of the Block is not acknowledged by the receiver before the time limit is reached, the Block is discarded.
ARQ_RETRY_TIMEOUT	The minimum time interval a transmitter SHALL wait before retransmission of an unacknowledged Block for retransmission. The interval begins when the ARQ block was last transmitted.



<u>Parameter</u>	<u>Description</u>
ARQ_SYNC_LOSS_TIMEOUT	The maximum time interval ARQ_TX_WINDOW_START or ARQ_RX_WINDOW_START SHALL be allowed to remain at the same value before declaring a loss of synchronization of the sender and receiver state machines when data transfer is known to be active. The ARQ receiver and transmitter state machines manage independent timers. Each has its own criteria for determining when data transfer is ‘active’. See <i>sections 6.3.4.6.2 and 6.3.4.6.3 in IEEE 802.16e standard</i> .
ARQRX PURGE TIMEOUT	The time interval the receiver SHALL wait after successful reception of a Block that does not result in advancement of ARQ_RX_WINDOW_START, before advancing ARQ_RX_WINDOW_START (see <i>section 6.3.4.6.3 in IEEE 802.16e standard</i> ).
ARQ_BLOCK_SIZE	The length (in octets) used for partitioning an SDU into a sequence of Blocks prior to transmission (see <i>section 6.3.4.1 in IEEE 802.16e standard</i> ).

The aforementioned parameters are communicated between BS and MS upon connection setup and do not change during the connection lifetime. Upon handover, the parameters, except from ARQ\_BSN\_MODULUS, which is constant, SHALL be synchronized between the Serving and Target BSs during the HO Preparation Phase.

#### 4.7.7.4.1.2 Synchronizing Downlink ARQ State after handover

From IEEE 802.16e perspective synchronization of the Downlink ARQ State means the following:

If MS received DISCARD message from the Serving BS but couldn't reply with acknowledgement, the MS SHALL send the acknowledgement to the Target BS. The MS may send the acknowledgements immediately after handover completion or may postpone it depending on the state of its internal timers.

The Target BS SHALL never transmit the ARQ blocks up to the one specified in the last DISCARD message from the Serving BS. The Target BS may re-transmit the DISCARD message (first transmitted by the Serving BS) immediately after handover or it may postpone the retransmission up until ARQ\_RETRY\_TIMEOUT after completion of handovers. If the Target BS does not receive the acknowledgement for the discarded blocks it SHALL retransmit DISCARD message at the intervals equal to ARQ\_RETRY\_TIMEOUT until it receives the acknowledgement.

If the MS had successfully received an ARQ block from the Serving BS but couldn't reply send the acknowledgement to the Serving BS, the MS SHALL send the acknowledgement to the Target BS. The MS SHALL send the acknowledgements immediately after HO completion or may postpone it depending on the state of its internal timers.

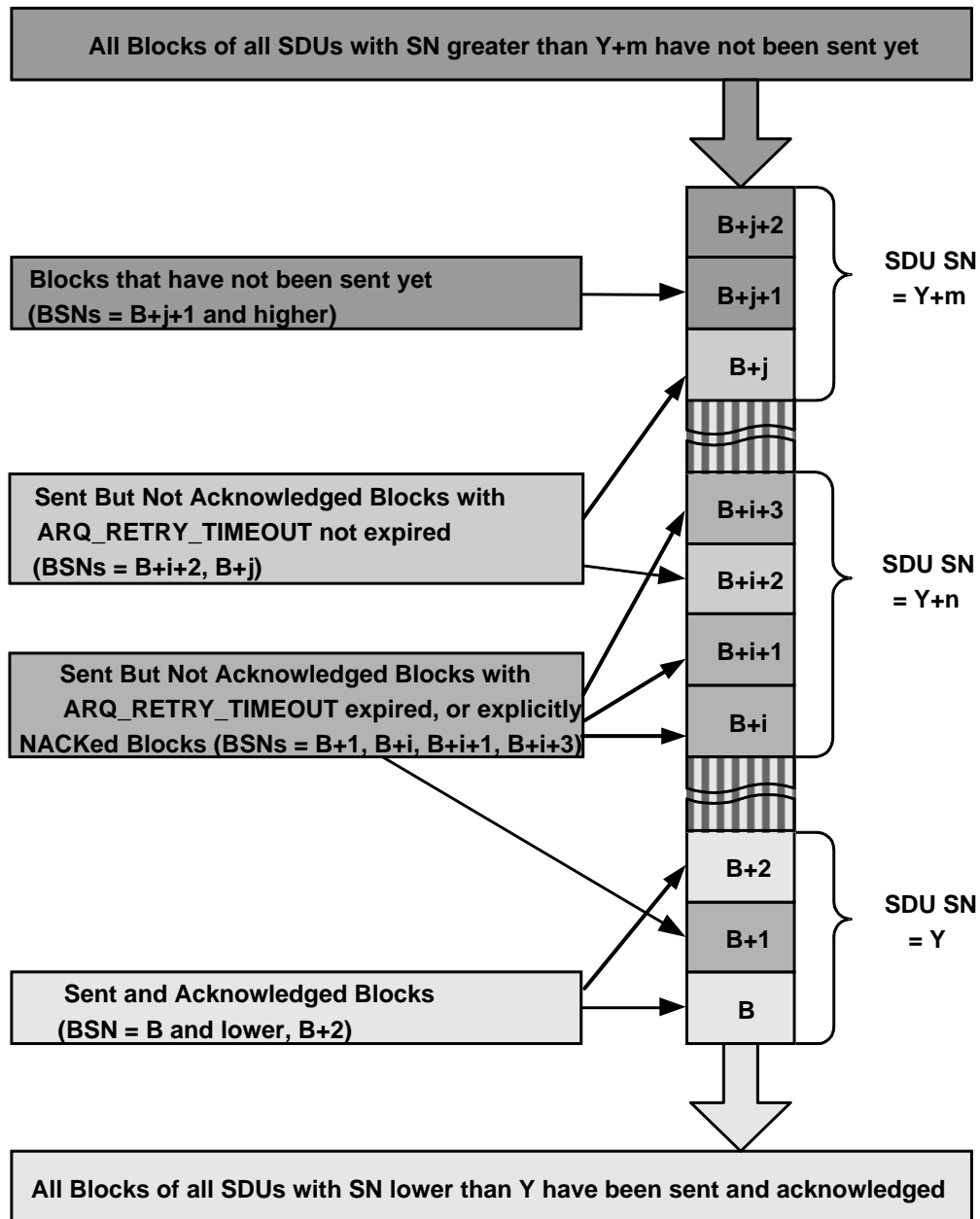
If the Serving BS has transmitted an ARQ block to the MS, but it was not acknowledged by the MS, the Target BS SHALL start retransmitting the ARQ block either immediately after HO completion or later, depending on the state of the internal timers, until it receives the acknowledgement from the MS.

If the Serving BS has transmitted an ARQ block to the MS, and the MS acknowledged it, the Target BS SHALL NOT transmit it again.

More details are available *IEEE 802.16e section 6.3.22.2.8.6.3*.

Notably the IEEE 802.16e standard does not require synchronizing timers associated with each state between Serving and Target BS (in the Serving and Target BSs respectively) because the operations of the ARQ State Machine never assume anything about the values of the timers associated with the peer ARQ State Machine.

A typical situation with the transmission buffer in the Serving BS, which may occur prior to MS leaving, is shown on the Figure 4-112. The transmission buffer in the Serving BS might be represented as sequence of Blocks labeled with BSNs. On the other hand each BSN belongs to the corresponding SDU labeled with SDU SN.



**Figure 4-112 – Example of per-SF Downlink Transmission Queue in Serving BS**

Each Block in the Transmission Queue might be in one of the following states:

**Done.** The Block has been transmitted and acknowledged. On the Figure 4-112 the Blocks with BSNs = B and lower, B+2 are in the Done State.

**Outstanding.** The Block has been transmitted but not acknowledged yet and ARQ\_RETRY\_TIMEOUT has not expired. On the Figure 4-112 the Blocks with BSNs = B+i+2 and B+j are in the Outstanding State.

**Waiting For Retransmission.** The Block has been transmitted but not acknowledged yet and ARQ\_RETRY\_TIMEOUT has expired. On the Figure 4-112 the Blocks with BSNs = B+1, B+i, B+i+1 and B+i+3 are in the Waiting For Retransmission State.

**Not Sent.** The Block has not been sent yet.

As it is explained in *802.16e section 6.3.4.6.2* A Block can also be in **Discarded** state, which means that its lifetime has expired (or the scheduling application has terminated the Block's lifetime). This state is not maintained per Block; instead the Transmitter maintains a pointer to the BSN specified in the last Discard Message. All Blocks with lower BSNs are in the **Discarded** State.

Synchronizing ARQ context means restoring this picture in the TBS. Upon handover Re-Entry, the SBS will convey the necessary information to the TBS. The information may include:

1. Mapping of Blocks onto SDUs (BSNs onto SDU SNs) in the Transmission Queue.
2. State of each Block in the Transmission Queue.
3. Start of the Tx ARQ Window (the first BSN in the Window)
4. The BSN specified in the last Discard Message if such a message has been sent.

#### **4.7.7.4.1.3 Synchronizing Uplink ARQ State after handover**

From IEEE 802.16e perspective synchronization of the Downlink ARQ State means the following:

The MS assumes that the network is capable of re-assembling the SDU parts, which may have been received by different Base Stations.

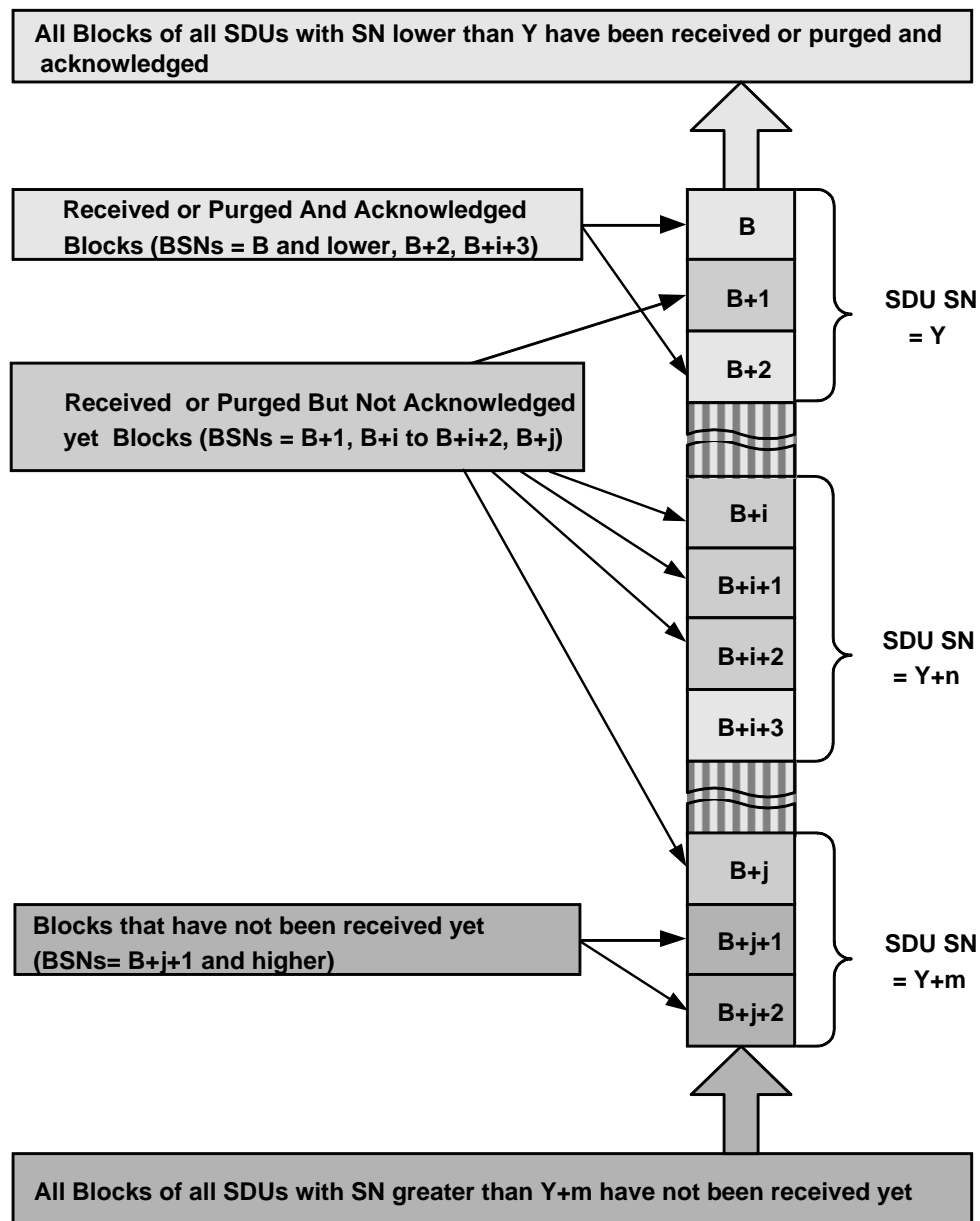
If the Serving BS has successfully received an ARQ block from the MS, but couldn't reply with acknowledgement to the MS, the Target BS SHALL send the acknowledgement to the MS. The Target BS may send the acknowledgements immediately after HO completion or may postpone it depending on the state of its internal timers.

If the MS has been transmitted an ARQ block to the Serving BS, but did not receive acknowledgement from the Serving BS, the MS SHALL start retransmitting it to the Target BS. It will do so either immediately after HO completion or later, depending on the state of the internal timers until it receives the acknowledgement from the MS.

If the MS has transmitted an ARQ block to the Serving BS, and received acknowledgement from the Serving BS, the MS SHALL NOT transmit it again to the Target BS upon HO completion.

More details are available *IEEE 802.16e section 6.3.22.2.8.6.3*.

A typical situation with the reception buffer in the Serving BS, which may occur prior to MS leaving, is shown on the Figure 4-113. The reception buffer in the Serving BS might be represented as sequence of Blocks labeled with BSNs. On the other hand each BSN belongs to the corresponding SDU labeled with SDU SN.



**Figure 4-113 – Example of per-SF Uplink Reception Queue in Serving BS**

Each Block in the Transmission Queue might be in one of the following states:

**Done.** The Block has been either received and acknowledged or purged and acknowledged. On the Figure 4-113 the Blocks with BSNs = B and lower, B+2, B+i+3 are in the Done State.

**Acknowledgement Pending.** The Block has been received or purged but not acknowledged yet. On the Figure 4-113 the Blocks with BSNs = B+1, B+i, B+i+1, B+i+2, B+j are in the Acknowledgement Pending State.

**Not Received.** The Block has not been sent yet. On the Figure 4-113 the Blocks with BSNs = B+j+1 and higher are in the Not Received State.

Synchronizing ARQ context means restoring this picture in the TBS. Upon handover Re-Entry the SBS will convey the necessary information to the TBS. The information will include:

1. Mapping of Blocks onto SDUs (BSNs onto SDU SNs) in the Reception Queue.

2. State of each Block in the Reception Queue.
3. Start of the Rx ARQ Window (the first BSN in the Window)
4. The last BSN to be purged.
5. The time when the SBS last heard from the MS.

#### 4.7.7.4.2 Downlink Data Integrity Methods

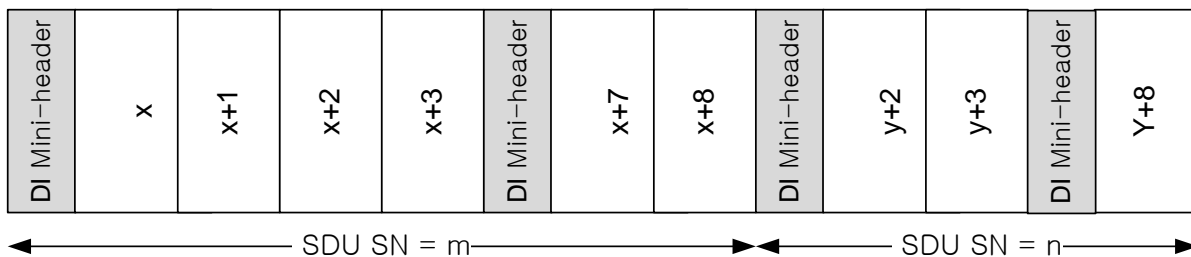
This section describes each specific method that can be applied for downlink data integrity with ARQ synchronization support during handover.

##### 4.7.7.4.2.1 BS Buffer Switching with ARQ State And Buffer Synchronization

This method acts on top of the BS Buffer Switching method described in Sec.4.7.4.3.1.3. This method employs an appropriate way for synchronization of ARQ state between the Serving and Target BS. The Serving BS SHALL consider all the ARQ blocks that are not acknowledged yet, at the time of receiving MOB\_HO-IND, as those that should be re-transmitted at the Target BS. The Serving BS SHALL forward those ARQ blocks to the Target BS before it forwards IP packets waiting for transmission to MS in its buffer. Those ARQ blocks which are forwarded between BSs SHALL be grouped into small Data Integrity packets as illustrated in the Figure 4-114. Each Data Integrity packet SHALL have special header -Data Integrity Mini-header- to include some ARQ-related information such as Starting\_ARQ\_BSN, packet length, etc.

Data Integrity Mini-header SHALL be inserted to distinguish groups of ARQ blocks which have contiguous block sequence numbers (BSNs) among them. Therefore, if there is discontinuity between the BSNs of any two adjacent groups of ARQ blocks or if IP packets to which any two adjacent groups of ARQ blocks which BSNs are discontinuous, a Data Integrity Mini-header SHALL be inserted between those groups.

For detailed information on Data Integrity Mini-header, refer to Table 4-109.



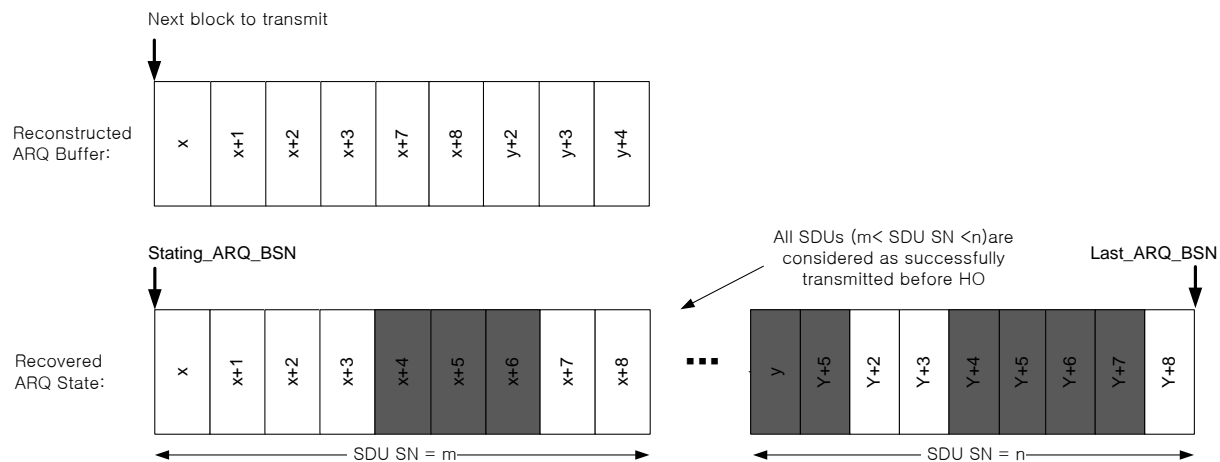
**Figure 4-114 – Data Integrity Packets to Forward ARQ Blocks (Example)**

Note: In the example above, the ARQ Blocks with sequence numbers  $x+4$ ,  $x+5$ ,  $x+6$ ,  $y$ ,  $y+1$ ,  $y+4$ ,  $y+5$ ,  $y+6$ ,  $y+7$  have been already acknowledged while MS resided in the Serving ASN. And, therefore, they are not included in the forwarding packets in the figure.

**Table 4-109 – Data Integrity Mini-Header**

Syntax	Size	Notes
FC	2 bits	Indicates the fragmentation state of the payload 00 = no fragmentation 01 = last fragment 10 = first fragment 11 = continuing(middle) fragment
BSN/FSN	11bits	Sequence number of the first block in the current payload
Length	11bits	Length of Data Integrity packet
Flag	8bits	Indicates the payload is in ARQ window or not 0 = Blocks are in ARQ window 1 = Blocks are not in ARQ window 2 ~ = reserved

The Target BS SHALL reconstruct ARQ buffer and related state machine for each flow, utilizing these Data Integrity packets and the ARQ state information delivered in the R6 HO-Cnf message. For detailed information regarding the ARQ state information used in this method, refer to Table 4-110 in the section 4.7.7.4.5.



**Figure 4-115 – Reconstruction of ARQ Buffers and State Machines at Target BS (Example)**

\*Note: In the example above, the ARQ Blocks with sequence numbers x+4, x+5, x+6, y, y+1, y+4, y+5, y+6, y+7 have been already acknowledged while MS resided in the Serving ASN, and are not sent by the Serving BS. Those blocks are pictured as black boxes in the forwarding packets in the figure.

#### 4.7.7.4.3 Uplink Data Integrity Methods

This section describes each specific method that can be applied for uplink data integrity with ARQ synchronization support during handover.

#### 4.7.7.4.3.1 SDU Reassembly Method

If ARQ State Synchronization is agreed between the Target and Serving BSs, then Uplink SDU Reassembly (either at the Data Path Anchor or at the Target BS) might be negotiated among the Target BS, Serving BS and Anchor ASN-GW. Uplink SDU Reassembly SHALL NOT be applied without ARQ Synchronization

One of the effects of the Uplink ARQ State synchronization explained in 4.7.7.4.1.3 is that parts of the uplink SDUs can be received in the Serving BS while the other parts can be received in the finally selected Target BS.

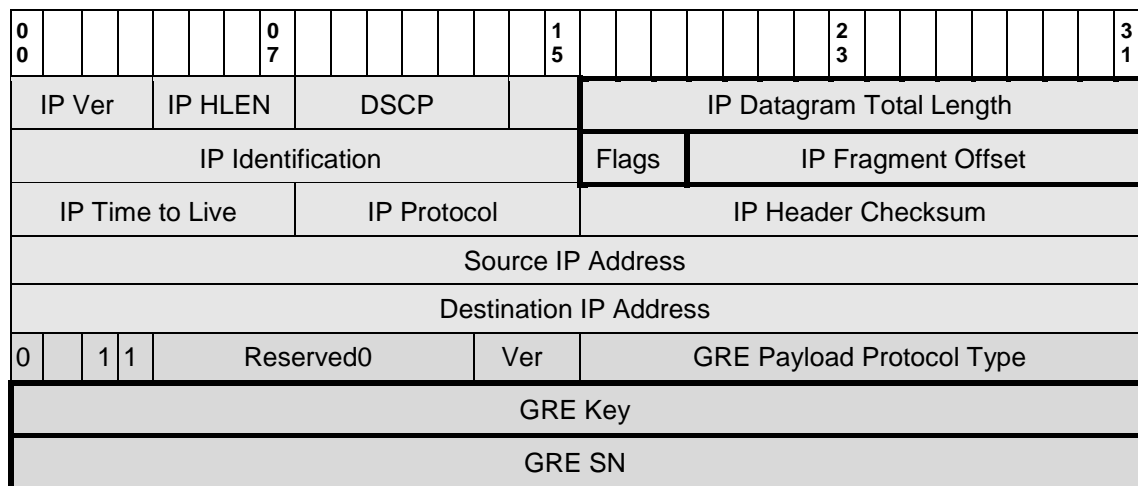
For example, consider delivery of the SDU with SN = Y+n on the Figure 4-113. The Blocks with BSNs = B+i and B+i+1 and B+i+2 have been received but not acknowledged in the Serving ASN, while the Block with BSN = B+i+2 can be received (if at all) only in the Target BS.

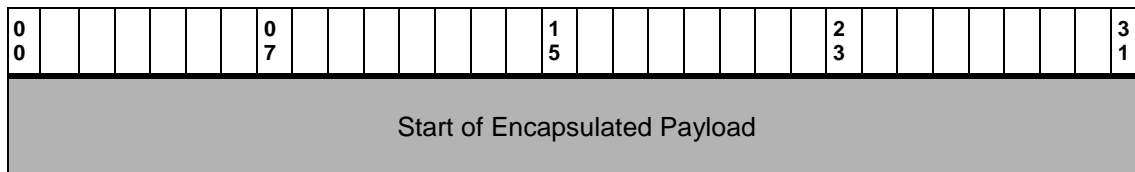
As it has been mentioned in 4.7.7.4.1.3, if the MS is notified that the network supports “Full Service And Operational State Transfer” then it assumes that the network is capable of reassembling the parts of the SDUs received in different ASNs (BSs).

##### 4.7.7.4.3.1.1 Uplink SDU Reassembly at Anchor ASN-GW

If the SDU Reassembly at the Anchor ASN-GW is used, the Serving BS will send upward the leftover uplink SDU fragments (e.g., fragments which consist of the ARQ Blocks with BSNs = B+i and B+i+1 and B+i+2 in the Figure 4-113) while the Target BS will send upward the rest fragments of SDUs (e.g., fragments which consists of the ARQ Blocks with BSN = B+i+3 in the Figure 4-113). The fragments will be delivered to the Anchor ASN where they need to be reassembled. Such reassembly adds however certain complexity, thus this functionality SHALL be negotiated during HO Preparation Phase as a separate optional feature. If the functionality is not agreed between the involved entities the uncompleted SDUs will be dropped after HO completion.

The reassembly functionality is modeled after IP reassembly described in the *RFC 791* and several fields used for IP reassembly are also used in this functionality. The fragments are organized as IP fragments of the encapsulating IP/GRE datagram. The inner datagram is treated as payload and its header is not affected. The fields relevant for Uplink SDU Reassembly at the Anchor ASN-GW are shown on the Figure 4-116.





**Figure 4-116 – Fields of the Outer Header Relevant for Uplink SDU Reassembly at Anchor ASN-GW**

The Flags field in the outer header control fragmentation. The meaning of the flags is the same as specified in the *RFC 791*

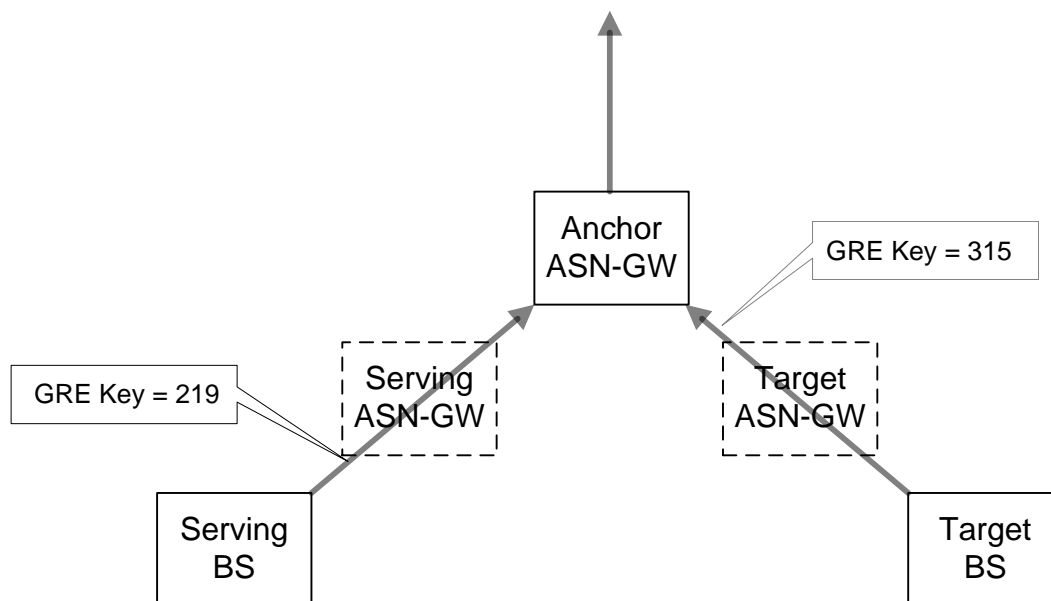
- Bit 0: reserved, must be zero
- Bit 1: 0 = May Fragment, 1 = Don't Fragment.
- Bit 2: 0 = Last Fragment, 1 = More Fragments.

The IP Datagram Total Length field specifies the length of the fragment. Contiguous Blocks transform into a single fragment.

The IP Fragment Offset specifies the fragment offset from the beginning of the SDU.

The aforementioned fields and their meanings are the same as specified in the *RFC 791*. However unlike the pure IP reassembly, the IP Identification field is not used to identify the datagram and the IP Source Address field is not used to identify the traffic source. Instead GRE Key and GRE SN respectively are used for that purpose.

Note that GRE Keys corresponding to the same Service Flow are different on the different branches of the Data Path Tree. The Figure 4-117 shows an example of such a tree.



**Figure 4-117 – Uplink Data Path Tree**

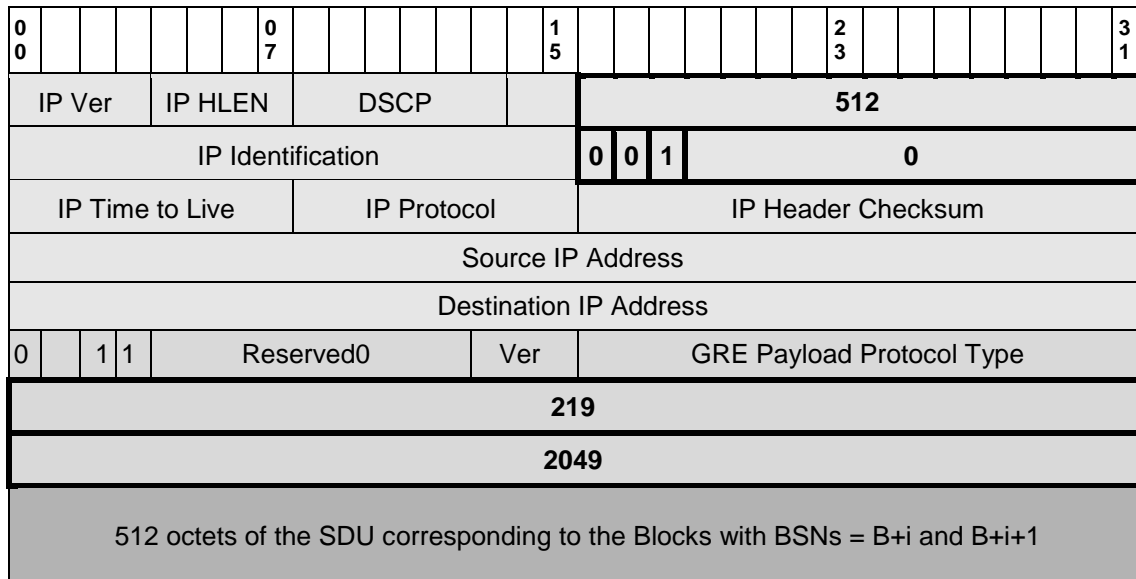
Assume the SDU with SN = Y+n on the Figure 4-113 is to be delivered to the Anchor ASN-GW from the Serving BS and Target BS. The corresponding Data Path Tree is shown on the Figure 4-117.

To make the explanation easier, assume Y+n = 2049. Assume also that the SDU length is 860 octets and the ARQ Block length is 256 octets. Thus the SDU is divided into four ARQ Blocks of which three (BSNs = B+i to B+i+2) are of 256 octets and the forth one (BSN = B+i+3) is of 92 octets.



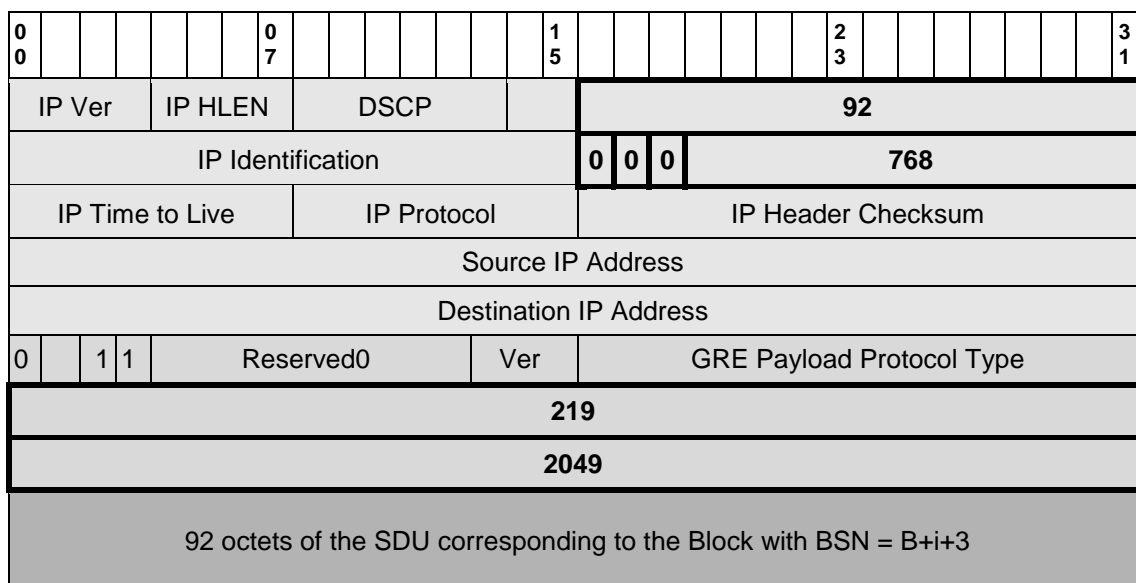
- 1 The two fragments sent from the Serving BS appear on the Figure 4-118 and Figure 4-119.

- 1 The first fragment, sent from the Serving BS (Figure 4-117) and corresponding to the Blocks with BSNs = B+i and  
2 B+i+1, appears on the Figure 4-118.



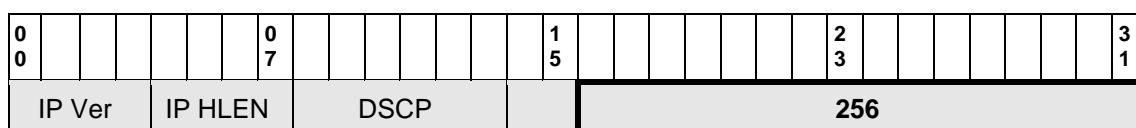
3 **Figure 4-118 – First Fragment Sent from the SBS**

- 4 The second fragment sent from the Serving BS and corresponding to the Block with BSN = B+i+3, appears on the  
5 Figure 4-119.

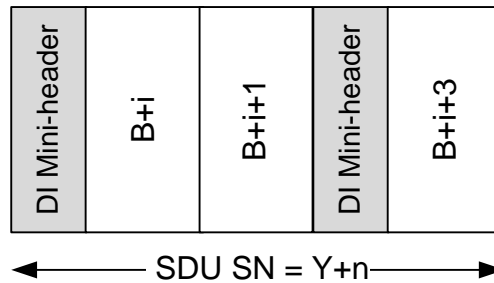


6 **Figure 4-119 – Second Fragment Sent from the SBS**

- 7 The fragment sent from the Target BS and corresponding to the Block with BSN = B+i+2 appears on the Figure  
8 4-120.







**Figure 4-121 – Data Integrity Packets to Forward ARQ Blocks (Example)**

#### 4.7.7.4.4 Auxiliary Use of SDU SN Report

The Serving and Target BSs and the MS may perform MS-Assisted coordination of DL transmission during handover as described in 802.16e section 6.3.22.2.8. The Target BS may signal to the MS on the intention to apply this procedure by using Bit #11 of ‘HO Process Optimization’ bitmask in the RNG-RSP message. The Serving BS may transmit ‘HO Process Optimization’ bitmask in the MOB\_BSHO-RSP or MOB\_BSHO-REQ messages.

For ARQ enabled connections, the MS may report to the Target BS the next ARQ BSN in the special header defined in 802.16e section 6.3.2.1.2.1.7. After reception of the header, the TBS SHALL resume transmission of the data of the corresponding DL Service Flow starting from the BSN specified in the header. The report from MS takes precedence over the ARQ Sync information received from the Serving ASN in case of mismatch.

#### 4.7.7.4.5 Informational Elements Added by this Functionality

Only Informational Elements related to the operation of the Data Integrity with ARQ Synchronization are described in this section. The Informational Elements related to the negotiation of the Data Integrity method are described in 4.7.7.5.

Since ARQ Synchronization is added on top of the basic Data Integrity functionality described in 4.7.7.3 new Informational Elements are added to those already described in 4.7.7.3.4.

HO Request delivers to the Target BS the ARQ State Machine parameters discussed in 4.7.7.4.1. The exact formats of the TLVs are specified in section 5.

Additional content of HO\_Cnf on top of baseline is shown here.

**Table 4-110 – Additions HO\_Cnf or Context Rpt From Serving BS to Target BS**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.
>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	CM	SFID associated with the Service Flow.  This TLV SHALL be included if SF Info is included in the transmitted message.
>>Pointer BSN (one or more)	5.3.2.381	O	A list of pointers to key positions in the transmission (if downlink) or reception (if uplink) BSN queue. The meaning of each pointer is determined by the internal field called “scope” (see section 6 for exact definition)  The first pointer indicates start of ARQ Window. If applicable another pointers may indicate Last BSN to Discard (if downlink) or Last BSN to Purge (if uplink).

IE	Reference	M/O	Notes
>>BSN ARQ State Bitmap (one or more)	5.3.2.382	O	Describes the state of each BSN in the transmission (if downlink) or reception (if uplink) queue.
>>SDU Info (one or more)	5.3.2.176	O	SDU Info for each SDU in the Transmission (downlink) or Reception (uplink) Queue.
>>>SDU SN	5.3.2.178	CM	The SN of the SDU.  This TLV SHALL be included if SDU Info is included in the transmitted message.
>>>Pointer BSN	5.3.2.381	O	Indicates the BSN of the first Block in the SDU
>>Data Path Info	5.3.2.45	O	
>>>Data Path ID	5.3.2.44	CM	
>>>Data Path Encapsulation Type	5.3.2.42	O	
>>>Data Path Type	5.3.2.47	O	
>>>Tunnel Endpoint	5.3.2.194	O	
>>>ARQ Window Info	5.3.2.448	O	If BS Buffer Switching is used, this TLV shall be included. This TLV delivers ARQ State information at the Serving BS, to the Target BS.
>>>>Starting ARQ BSN	5.3.2.449	CM	Indicates the ARQ_TX_WINDOW_START(Transmitter) or ARQ_RX_WINDOW_START(Receiver).  This TLV SHALL be included if ARQ Window Info is included in the transmitted message.
>>>>Last ARQ BSN	5.3.2.450	CM	Indicates the ARQ_TX_NEXT_BSN(Transmitter) or ARQ_RX_HIGHEST_BSN(Receiver).  This TLV SHALL be included if ARQ Window Info is included in the transmitted message.
>>>>Valid ARQ BSN	5.3.2.451	CM	Indicates the BSN of the NOT Discarded ARQ Block in the ARQ window. (Downlink SF only)  This TLV SHALL be included if ARQ Window Info is included in the transmitted message.
>>>>Reset Status	5.3.2.452	CM	Indicates whether ARQ reset was pending at the Serving BS before HO.  This TLV SHALL be included if ARQ Window Info is included in the transmitted message.

#### 1 4.7.7.5 Negotiating Data Integrity Method

- 2 HO related Data Integrity Methods are negotiated per service flow during the HO Preparation Phase. The entities
- 3 involved in the Handover and Data Path Pre-Registration transactions negotiate the options among them.
- 4 The same data integrity scheme SHALL be applied to all the chosen SFs of the same MS.

A Data Integrity Capability TLV is defined and should be passed from involved BSs to Anchor ASN-GW using Handover and Data Path Pre-Registration transactions.

Upon handover, the Serving BS passes its own Data Integrity Capability TLVs to Target BS through HO Request message. Data Integrity Applied TLV is included in this message to indicate whether the DI method should be applied to a specific service flow or not. And DI method is unavailable to a service flow by default. The Target BS should pass the mutual section of Data Integrity Capability TLVs of serving BS and itself to Anchor ASN-GW using Data Path Pre-Registration Request eventually. The Target BS SHALL notify the Anchor ASN-GW of its own selection for data integrity method using a Path\_Pre-Reg\_Req message. The Anchor ASN-GW SHALL decide which Data Integrity Method (s) should be used based on its local policy and Service Flow QoS information, if the BS Buffer Switching method is not chosen by the Target BS. If the BS Buffer Switching method is chosen by the Target BS and supported by the Anchor ASN-GW, then the Anchor ASN-GW SHALL not change the decision. The final selection of Data Integrity Method TLV for each service flow should be passed to Target BSs using Data Path Pre-Registration Response messages. The Target BS then passes the final selection of Data Integrity Method TLV to Serving BS through HO Response message.

The Data Integrity Capability TLV has been defined in 5.3.2.378. The Data Integrity Method TLV has been defined in 5.3.2.379. Some options can be set together but some not. Per-SF Selective Multi-Unicasting and Buffering with Delivery on Demand cannot be selected together in the final decision. Reassembly of Uplink SDUs at the Anchor BS can be selected only if ARQ Synchronization for uplink is selected. ARQ Synchronization may be selected independently of the data delivery method used (Multi-Unicasting or Buffering with Delivery on Demand).

The Table 4-111 shows placing of Data Integrity Capability TLV and Data Integrity Method TLV in the structure of Path Pre-Registration Request/Response and HO Request/Response message.

**Table 4-111 – Data Integrity Method TLV in Path\_Pre-Reg\_Req and HO Req**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.
>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	CM	SFID associated with the Service Flow.  This TLV SHALL be included if SF Info is included in the transmitted message.
>>>Data Integrity Method	5.3.2.379	O	Data Integrity Method bitmask indicating the methods selected by the Target-BS.
>>>Data Path Info	5.3.2.45	O	
>>>>Data Path ID	5.3.2.44	CM	
>>>>Switching Data Path ID	5.3.2.383	O	It shall be used when the Data Integrity method of BS buffer switching is selected. This indicates GRE Key for data path which shall be used to forward data packets buffered at the Serving BS.
>>>>Data Integrity Applied	5.3.2.380	O	This TLV is used to indicate whether the Data Integrity Method should be applied to a specific Service Flow or not ( <i>HO Req</i> ).
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

IE	Reference	M/O	Notes
>Data Integrity Capability	5.3.2.378	O	Serving-BS's Data Integrity Capability ( <i>HO Req</i> ) or mutual Data Integrity Capability of Serving-BS and Target-BS ( <i>Path_Pre-Reg_Req</i> ).

**Table 4-112 – Data Integrity Method TLV in Path\_Pre-Reg\_Rsp and HO Rsp**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.
>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	CM	SFID associated with the Service Flow
>>Data Integrity Method	5.3.2.379	O	Indicate the authorized Data Integrity Method bitmask.
>>>Data Path Info	5.3.2.45	O	
>>>>Data Path ID	5.3.2.44	CM	
>>>>Switching Data Path ID	5.3.2.383	O	It shall be used when the Data Integrity method of BS buffer switching is selected. This indicates GRE Key for data path which shall be used to forward data packets buffered at the Serving BS.

## 4.8 CSN Anchored Mobility Management

### 4.8.1 Introduction

This section describes the CSN Anchored Mobility Management procedures. The term “mobility” means CSN anchored mobility within the context of this section. The procedures described here are categorized into network access based on IPv4 and IPv6. IPv4 support is mandatory for the MS and network. IPv6 support is optional for the MS and network.

The IPv4 network access and mobility management is either performed with Proxy Mobile IPv4 (PMIP4), Client Mobile IPv4 (CMIP4), or Proxy Mobile IPv6 (PMIP6) when its IPv4 mobility support functionality is enabled [93]. PMIP4 and PMIP6 (when IPv4 mode is enabled) require DHCPv4 support at the MS and network. IPv4 mobility support is required. The network SHALL support the DHCP and CMIP4 procedures described in this section for IP address acquisition. The MS SHALL support either the DHCP or CMIP4 procedures described in this section for IP address acquisition. The network and MS SHALL support the DHCP procedures described in [24] for bootstrapping configuration information to the MS after IP address acquisition.

Simultaneous PMIP4 and CMIP4 operation by the same mobile is not supported in this specification.

The IPv6 network access and mobility management is performed either with Client Mobile IPv6 (CMIP6) using authentication protocol ([71]), or with Proxy Mobile IPv6 (PMIP6) [81]. An IPv6 MS MAY rely on address autoconfiguration or DHCPv6 for its IPv6 address acquisition. The access network that provides IPv6 service SHALL support both the IPv6 configuration through stateless address autoconfiguration, and one of the DHCP6 options, either Proxy or Relay mode, regardless of the mobility service assigned to the MS. Simultaneous PMIP6 and CMIP6 operation is not supported for the same MS. If an MS with an active PMIP6 session attempts the CMIP6 BU registration, the HA/LMA SHALL respond with BA message setting the error code to value 133 (Not home

agent for this mobile node). The network or the MS MUST NOT trigger network exit or network rejection procedure in this case.

A NAP operator may assign addresses from private address space range to the functional entities in its access network. The CSN operator may choose to assign addresses from the same private address space to the MSs. Since CSN and ASN are independent administrative domains and are not synchronizing their usage of private address space, it may happen that the same address that the CSN assigned to a particular MS is also assigned to the ASN GW to which this MS is attached. Some ASN entities, like DHCP Proxy, are originating IP datagrams destined to MSs. If the ASN entity originating a datagram destined for the MS and the MS is assigned the same private IP address as the MS, then the datagram would have the same IP address in both the destination and source address fields in the IP header.

In order to prevent this problem, the entities in the NAP's network that originate datagrams towards the MS SHALL be configured with a public IP address. This will prevent the problem of the address collision. Entities affected by this requirement include the DHCP Proxy and the entity acting as a default router for the MS (which originates Router Advertisements). Those entities may have additional private addresses assigned but they SHALL use their public IP address as a source IP address when originating datagrams towards a MS.

## **4.8.2 Proxy MIP4 R3 Mobility Management**

The proxy Mobile IPv4 procedure is entirely done in the network and the MS is agnostic to the related procedures. There are certain events that take place with the MS e.g., MS requesting an IP address assignment at the connection setup time or the MS performing an handover across BS boundaries that require relocation of the network layer anchor point (e.g., change of CoA) that MAY serve as a trigger for Proxy Mobile IPv4 transactions in the network.

### **4.8.2.1 Proxy MIP4 Connection Setup Procedure**

The basic connection setup procedure using PMIP4 is shown in Figure 4-122 (DHCP Proxy) and Figure 4-75 (DHCP Relay). The node requirements to support the connection setup are described as follows.

During the initial network entry, PMIP4 Client, DHCP proxy or relay function, Authenticator and FA are all collocated.

#### **4.8.2.1.1 MS Requirements**

The MS SHALL support the DHCP client function as defined in [24]. In order to acquire an IPv4 address, the MS SHALL send a DHCPDISCOVER message to the network over the initial service flow. Upon receiving the DHCPOFFER message from the network, the MS SHALL follow the procedures defined in [24] to select and configure an IPv4 address included in the DHCPOFFER message.

The MS SHALL also refresh the DHCP Lease Time based on the  $T_1$  and  $T_2$  parameters received in the Op Codes 58 and 59 in [25].

#### **4.8.2.1.2 DHCP proxy/relay/server Requirements**

For CSN anchored mobility, ASN-GW SHALL support DHCP Proxy. ASN-GW MAY also support DHCP Relay.

Inter-ASN handovers are not supported between DHCP Proxy and Relay ASNs.

NOTE: The DHCP Proxy is a DHCP Server from the perspective of the MS.

##### **4.8.2.1.2.1 DHCP Proxy Requirements**

Upon receiving a DHCPDISCOVER message from the MS, the DHCP proxy MAY ignore the "chaddr" field in the DHCP header and use the pseudo NAI associated with the ISF data path tunnel (i.e., R6) over which the DHCP message was received as the identity of the MS to acquire a HoA. This is feasible without any additional Option in the DHCP message since the DHCP proxy is collocated with the Anchor ASN. This is done to prevent MAC address spoofing by a rogue MS.

The DHCP proxy prompts the collocated PMIP4 client to initiate the PMIP4 procedures. If there had been no previously received HoA during the authentication phase, the PMIP procedure will acquire a HoA from the home agent, else the HoA obtained during authentication is sent in the PMIP registration request.



In case the DHCP proxy determines that the MS has included a MAC address in the chaddr field of the DHCP discover message that is not matching with the known MAC address associated with the data path (i.e., R6) over which the DHCP message is received, the DHCP proxy MAY consider the following:

- A rogue MS trying to spoof MAC address. In this case, the DHCP proxy MAY inform the DPF to initiate data path (i.e., R6) teardown.

Upon receiving a response from the PMIP4 Client with an indication of successful PMIP4 registration, the DHCP proxy SHALL extract the HoA that is assigned to the MS and respond back to the MS with a DHCPOFFER message setting the Your IP address field to the received HoA, Server IP address field to the IP address of the DHCP proxy, and Transaction ID copied from the DHCPDISCOVER message. DHCP proxy SHALL set the Subnet option to the value 255.255.255.255 and SHALL set the Router option to the IP address of the DHCP proxy. It MAY set the Domain Name Server option to the address of the DNS server when received in the RADIUS Access-Accept packet or Diameter WDEA command from the AAA server. The DHCP proxy SHOULD send a single DHCPOFFER message.

If a DHCP Decline message is received, the DHCP proxy MUST not establish an IP session and SHALL release any existing Layer 3 session associated with this DHCP transaction.

For the subsequent DHCPREQUEST with the assigned IPv4 address (HoA), the DHCP proxy SHALL respond back to the MS with DHCPACK. In the DHCPACK message the DHCP proxy SHALL set the address lease time parameters ( $T_1$  and  $T_2$  correspond to RENEWING and REBINDING state timers in the MS) as follows as default setting:

- $T_1 = 0.5 * \text{Lease Time}$
- $T_2 = 0.875 * \text{Lease Time}$

However, these values are configurable based on local network policy for optimization of network resources.

In order to reduce frequent address renewal messaging over the air, the Lease Time SHOULD be set as reasonably large value.

In order to facilitate seamless mobility movement from a MS's perspective, all DHCP proxy entities within a NAP or at least within a group of ASNs belonging to a NAP which support inter-ASN mobility movement SHALL use the same operator-configured public IP address as the server identifier and the source IP address in the DHCP messages sent to the MS. This will make it looks like the MS is communicating with the same DHCP proxy entity at all time, even after the handoff to a different ASN, therefore guarantees the continuity of the DHCP state machine. This public IP address SHALL be reserved for DHCP proxy entities only and SHALL NOT be used by any other functional entities within the NAP. This public IP address SHALL NOT be propagated within the ASN routing domain in case there is a need to turn on routing protocol in the user data plane.

#### 4.8.2.1.2.2 DHCP Relay Requirements

The DHCP relay SHALL support the procedures defined in [25], [44] and [60] and [69].

The DHCP relay SHALL handle all DHCP messages sent by the MS to the broadcast IP address.

The DHCP relay is configured with the DHCP server address during the MS authentication. The AAA server MAY send the address of the DHCP server in the RADIUS Access-Accept message or Diameter WDEA command. The DHCP relay SHALL use this address to relay the DHCP messages from the MS to the DHCP server.

Upon receiving a DHCPDISCOVER message from the MS, the DHCP relay SHOULD verify the "chaddr" field in the DHCP header matches the MS MAC address associated with the R6/R4 over which the DHCP message is received. This is feasible without any additional option in the DHCP message since the DHCP relay is collocated with the Anchor ASN-GW. This is done to prevent MAC address spoofing by a rogue MS.

In case, the DHCP relay determines that the MS has included a MAC address in the chaddr field of the DHCPDISCOVER message that does not match with the known MAC address associated with the R6/R4 over which the DHCP message was received, the DHCP relay MAY consider the following action:

- A rogue MS trying to spoof MAC address. In this case, the DHCP relay MAY inform the DPF to initiate R6 teardown.

After determining the NAI (defined in subclause 4.4.1.3.1) to be used for the request, the DHCP relay SHALL add the relay agent option 82/6 to the original DHCP message and sets the Subscriber-ID suboption to the NAI used for MIP (defined in subclause 4.4.1.3.1) associated with MS. If there is a secure communication channel between the DHCP relay and the DHCP server, the relay and server MAY choose to omit the authentication suboption. The steps describing the processing action of the DHCP relay with respect to the authentication suboption are described in 4.3.6.2.

If a DHCP Decline message is received, the DHCP Relay SHALL forward the message on to the DHCP Server.

The messaging between the DHCP relay and DHCP server is transported over R3 interface.

When DHCP relay receives the DHCPOFFER message from the DHCP server, it SHALL relay it to the MS. If the DHCP server included the authentication suboption in the relay agent option, the DHCP relay SHALL validate it before relaying the DHCPOFFER to the MS.

The DHCP relay behavior for handling DHCPREQUEST or DHCPDECLINE from the MS is same as in the case of DHCPDISCOVER.

When DHCP relay receives the DHCPREQUEST message from the MS, it SHALL prompt the PMIP4 client to initiate MIP4 registration procedures and pass the requested IPv4 address (yiaddr in DHCP header of the DHCPREQUEST) and the HA information to the PMIP4 client. The PMIP4 client SHALL perform the registration with the FA and HA on behalf of the MS. The PMIP4 client SHALL inform the DHCP relay with the MIP4 registration result. Upon receipt of such indication, the DHCP relay SHOULD relay the DHCPREQUEST message with the MIP registration result encapsulated in the vendor specific relay agent suboption code 1 as defined below to the DHCP Server. If this suboption is not sent to the DHCP server and the MIP registration indicates a failure, the DHCP relay SHALL NOT forward the DHCPREQUEST message to the DHCP server and the network SHALL perform an exit for the corresponding MS. When DHCP relay receives the DHCPACK message from the DHCP Server, it SHALL relay the DHCPACK message to the MS.

Since AAA can assign different HAs (e.g., when dynamically assigning HA from a pool) and each HA handles different MS subnets, the assigned HA needs to be passed to DHCP server to allow choosing the matching MS address pool. DHCPDISCOVER and DHCPREQUEST from MS SHOULD include HA IP address in same vendor specific relay agent suboption code 2 as define below to the DHCP Server.

The DHCP relay SHOULD support vendor specific relay agent suboption as defined in RFC 4243, which is included here as a reference:

```

+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| Code   | Length | Enterprise Number1 |
+-----+-----+-----+-----+-----+-----+-----+
|                               | DataLen1 |
+-----+-----+-----+-----+-----+-----+
\                               Suboption Data1                               \
+-----+-----+-----+-----+-----+-----+-----+
|                               Enterprise Number2                               |
+-----+-----+-----+-----+-----+-----+-----+
| DataLen2 | Suboption Data2 |
+-----+-----+-----+-----+-----+-----+-----+
\                               \
.                               .
.                               .
+-----+-----+-----+-----+-----+-----+-----+
    
```

Where Code is 9, Length is variable, indicating the length of subsequent data in number of bytes. Enterprise number1 is “24757” for WiMAX. DataLen1 is variable, indicating the length of Suboption Data1 in number of bytes. Suboption Data1 is coded as a sequence of sub-TLVs. In this release, only 2 sub-TLVs are defined as follows. Also both sub-TLVs can be sent independent of each other, and the HA IP address sub-TLV is expected to be sent both in DHCPDISCOVER and DHCPREQUEST while MIP4 registration result sub-TLV only included in DHCPREQUEST.

Subopt-code (WiMAX DHCP relay agent subopt code): 1 – MIP4 registration

1 result  
2 Length:1  
3 Value: MIPv4 registration result code as defined in RFC3344  
4 Subopt-code (WiMAX DHCP relay agent subopt code): 2 - HA IP address  
5 Length: Variable(either 4 or 16)  
6 Value: IP address of HA

7  
8 The DHCP relay SHALL intercept the DHCP renewal and release messages, verifying the content of the message. If  
9 R3 is not secured (e.g., by IPSec), the DHCP relay SHALL add the relay agent authentication suboption to the  
10 message before relaying it to the DHCP server.

11 For Dynamic HA assignment when both visited and home DHCP server addresses are available, DHCP relay  
12 SHALL select which DHCP server to be used, based on the local policy.

#### 13 **4.8.2.1.2.3 DHCP Server Requirements**

14 The DHCP server SHALL support the procedures defined in [25], [44]and [60] and [69].

15 The DHCP server SHALL be located in the CSN. The DHCP server and the HA SHALL be located in the same  
16 CSN.

17 During the initial address assignment and the subsequent address renewals, the DHCP server receives DHCP  
18 messages from the DHCP relay in the ASN. If the message received by the DHCP server includes the relay agent  
19 authentication suboption [69], the DHCP server SHALL validate it and also include the relay agent authentication  
20 suboption in its response, so that DHCP relay can do the same. If the DHCP server needs to obtain a DHCP-RK to  
21 validate the authentication suboption messages, the server sends a AAA Access-Request packet to the local AAA  
22 server or in the Case of Diameter, the DHCP server SHALL support the WiMAX DHCP Diameter Application and  
23 send a WDHCP command to the HAAA.

24 In the case of RADIUS, the DHCP server SHALL include the Message Authenticator (80) attribute used to integrity  
25 protect the Access-Request packet. The value of the Message-Authenticator attribute is set in accordance with the  
26 computation specified in [40].

27 When sending the RADIUS Access-Request packet or the WDHCP command to the AAA server, the DHCP  
28 server SHALL include the following attributes:

- 29 • The RADIUS NAS-Identifier attribute or the Diameter Origin-Realm AVP set to the FQDN of the DHCP  
30 server originating the request.
- 31 • The NAS-IP-Address attribute or the Diameter Origin-Host AVP set to the IPv4 or IPV6 address of the  
32 DHCP server.
- 33 • The DHCPMSG-Server-IPv4 set to the address contained in the DHCPDISCOVER message if the DHCP  
34 server address in the DHCPDISCOVER message is different from the address contained in the DHCPv4-  
35 Serverattribute.
- 36 • The DHCP-RK-Key-ID set to the value of the Key-ID received as part of the authentication suboption in  
37 the DHCPDISCOVER message.

38 If the DHCP message received by the DHCP server includes the vendor specific relay agent suboption as defined in  
39 section 4.8.2.1.2.2 containing the MIP registration result, the DHCP server SHALL check it and include the  
40 appropriate reason in its response if the MIP registration has failed. The DHCP server SHALL process the  
41 DHCPDISCOVER and DHCPREQUEST messages sent by the relay agent and the DHCP Client according to  
42 [25]and [60].

43 All messages originated by the DHCP server SHALL always include the server identifier option set to its own IP  
44 address.

45 In the case when DHCP lease time expires, the DHCP server MAY inform the HA that the HoA assigned to an MS  
46 has expired. In response, the HA MAY send Registration Revocation to the FA, so that the PMIPv4 client and related

resources can be released. If FA-HA AE is required, the HA SHALL select the most recent FA-HA key that was used by the FA.

Synchronization between the DHCP server and the HA is not specified by this document and is left as an implementation option.

#### 4.8.2.1.3 PMIP4 Client Requirements

Upon receiving an internal trigger from a DHCP proxy or relay function, the PMIP4 Client SHALL extract the user info from the trigger. With the extracted user info, the PMIP4 Client SHALL attempt to locate the PMIP4 Context that is cached in the Authenticator ASN (PMIP4 Client is collocated with the Anchored Authenticator). If the associated PMIP4 Context is found in the local cache, the PMIP4 Client SHALL proceed with the Mobile IPv4 registration process. Otherwise, the PMIP4 Client SHALL notify the DHCP proxy or relay function that the context for the corresponding NAI is missing.

The PMIP4 Context is established at the Anchor Authenticator during Device/User Network Access Authentication and Authorization procedures (see section 4.4.1).

After identifying the PMIP4 Context, the PMIP4 Client SHALL extract the following information from the Context:

- Identity@realm or the PMIP-Authenticated-Network-Identity, when present;
- MN-HA key(s) and MN-HA-SPI-PMIP4<sup>14</sup>;
- Home Agent address(es) to be used for this registration;
- HoA (if any);
- Registration Lifetime.

It is assumed that initially the PMIP4 Client is collocated with the FA in the same network element (i.e. ASN-GW). The Registration Lifetime is the lifetime of the Mobile IP session permitted by the FA. The value is assigned by the FA (initially co-located with the PMIP4 Client) in the PMIP4 Context. The PMIP4 Client SHALL generate a Mobile IPv4 Registration Request (RRQ) as per [48]. For CMIP and PMIP co-existence network, the RRQ from PMIP client contains a value of the SPI = SPI-PMIP4, associated with the PMIP MN-HA that was received during the EAP based Device/User Network Access Authentication and Authorization. This value of SPI is used to indicate the mobility mode of this MS and direct MIP signaling to PMIP client. The RRQ SHALL also contain the NAI extension carrying the PMIP-Authenticated-Network-Identity or undecorated Outer-Identity and the realm of the HCSN of the user established during Device/user Network Access obtained from the PMIP4 Context. If the PMIP4 context contains the HoA (assigned by the Home AAA and delivered through DHCP proxy) the RRQ SHALL include this HoA. Otherwise, the HoA segment in MIP RRQ need be set to 0. The Authorization-Enabling extension in this message SHALL be MN-HA AE.

During network access authentication, there may be two HA addresses downloaded to the Authenticator, as well as two MN-HA keys for PMIP4. The PMIP4 Client SHALL use a local policy to determine which HA to send the RRQ to, and the corresponding MN-HA key to use.

Upon receiving a MIP4 Registration Reply (RRP) from the Home Agent, the PMIP4 Client SHALL authenticate the message by processing the MN-HA AE and FA-HA AE. If authentication is successful and if the message passes replay verification, the PMIP4 Client SHALL inspect the RRP for any error codes. If the reply code is set to 0 indicating successful registration, the PMIP4 Client SHALL extract the HoA information from the RRP and notify the DHCP proxy with an indication of MIP4 registration success including the assigned HoA address(assigned HoA). Otherwise, the PMIP4 Client SHALL notify the DHCP proxy indicating the failed operation to acquire an IPv4 (HoA) for the Outer-Identity.

#### 4.8.2.1.4 FA Requirements

FA SHALL operate as defined in [48] and [50].

---

<sup>14</sup> 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.

To identify the radio access technology (RAT) used in the ASN, the FA SHOULD append to the RRQ the PMIP Access Technology Type Extension defined in PMIP4 [92] to indicate which access type is being used, before relaying the RRQ to the HA.

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 HA. Also, the FA SHALL include the Revocation Support Extension as per [50] so that registration revocation can be performed when needed. In the Revocation Support Extension, the FA SHALL set the I-bit to 0. If FA-HA AE is used to protect these messages, the FA SHALL validate the FA-HA AE in the RRP before forwarding the same to the PMIP4 client.

FA SHALL fetch the necessary MIP keys from the Authenticator.

FA relocation in this release SHALL only be supported between the AnchorDPF and serving ASN/ASN-GW.

#### 4.8.2.1.5 HA Requirements

The HA SHALL process Mobile IPv4 messages as per [48] and [50]. The PMIP4 Client populates the HA address in the RRQ with the HA address of the HA that receives the RRQ (HA assignment happens via the HAAA during the EAP based Device/User Network Access Authentication and Authorization procedure, see section 4.4.1). The HA could be either in visited network or the home network.

Upon receiving the MIP4 RRQ message the HA SHALL perform replay verification as per [48]. If replay verification succeeds, the HA SHALL extract the NAI included in the NAI extension. Since this is an initial connection setup, the HA does not have a Binding Cache Entry (BCE) for the user, as identified by the NAI extracted from the NAI extension. The HA SHALL perform AAA transactions as described below to fetch the MN-HA key and if needed, HA-RK key. Note that the HA is agnostic to PMIP4 vs. CMIP4.

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 described in section 4.3.5. The HA SHALL validate the MN-HA AE and FA-HA AE in the received RRQ. Considering successful validation, the HA SHALL assign an IPv4 address to the user (Outer-Identity) if not included in the RRQ, and admit the binding and the associated keys in the BCE. If the RRQ contains a non-zero HoA value, and that HoA is not supported another, the HA SHALL reject the registration request and send code 129 in RRP (administratively prohibited).

If properly authenticated RRQ contains HoA that belongs to an existing session but a new MIP NAI, HA action depends upon an authority assigning HoA:

If HoA is assigned by AAA (DHCP Proxy configuration), remove the existing session with the same HoA, and accept the new session with this HoA.

If HoA is assigned by DHCP server (DHCP Relay configuration), remove the existing session with the same HoA, and accept the new session with this HoA.

Otherwise, the HA SHALL send a RRP back to the source address of the received RRQ. The RRP SHALL include the assigned HoA. The other fields of the RRP SHALL be set as per [48].

If the HA receives a Registration Request that does not include an MN-HA authorization extension, the HA SHALL silently discard the Registration Request.

If a properly authenticated *MIP RRQ* contains a MIP NAI already assigned to an existing MIP binding, but the *MIP RRQ* requests a specific HoA which does not match the existing binding, the HA shall remove the existing binding and establish the new binding per the triggering *MIP RRQ*.

If a properly authenticated *MIP RRQ* contains a MIP NAI already assigned to an existing MIP binding and the *MIP RRQ* requests a specific HoA which matches the existing MIP binding or no specific HoA was requested in the triggering *MIP RRQ*, the HA shall conditionally:

- Treat the *MIP RRQ* as a renewal of the existing binding if, as part of validating the *MIP RRQ*, an Access-Accept is received from the AAA, with device session state (e.g. WiMAX-Session-Id, CUI) which matches the existing binding

- Remove the old binding and establish a new binding per the triggering *MIP RRQ* if, as part of validating the *MIP RRQ*, an Access-Accept is received from the AAA with device session state (e.g. WiMAX-Session-Id, CUI) which does not match the existing binding

Note: Aside from otherwise documented rules, no further specific HA handling is required for the case of a properly authenticated *MIP RRQ* which requests no specific HoA and yet a binding existing for the same MIP NAI. This ensures consistent behavior between subscribers provisioned for static HoA with those provisioned for dynamic HoA, since given the static HoA case with constant MIP NAI, the *MIP RRQ* message for a MIP Renewal looks exactly the same as the *MIP RRQ* message for MIP establishment.

The following general rules apply whenever the HA establishes or removes a MIP binding:

- When the HA removes a binding (either because the HA detects the binding is stale or because the binding times out) and if the HA is performing Accounting for the binding, the HA SHALL generate an *Accounting-Stop* for the old binding, including the old WiMAX-Session-Id and any other relevant details matching the old binding (e.g. CUI, volume counts, IP address etc). Since the binding is being removed, all processing options from the old binding (e.g. filter rules etc) also no longer apply. If the binding is being removed due to expiry or due to the binding being proven stale based on a properly authenticated *MIP RRQ* for a new MIP NAI, the HA SHALL also send a MIP Revocation for the old MIP NAI to inform the FA/MN that the old MIP binding is no longer valid. If the HA attempts a MIP revocation, the HA shall remove the old binding regardless of whether the MIP revocation attempt succeeds or fails.
- Whenever the HA establishes a new binding (whether because of recovery after removal of stale binding or normal binding setup), the HA shall apply the processing options (e.g. filter rules etc) from the new Access-Accept and generate an *Accounting-Start* for the new binding, including the new WiMAX-Session-Id (received in the new AAA -> HA Access-Accept) and any relevant details matching the new binding (e.g. CUI, IP address etc).

Whenever a properly authenticated *MIP RRQ* indicates that an existing binding is stale, the HA shall follow the above rules to remove the existing binding and to establish a new binding per the new *MIP RRQ*.

For cases where the MIP NAI from the triggering *MIP RRQ* does not match the old binding, the HA shall not include device session information about the old binding (i.e. WiMAX-Session-Id, old CUI value etc) in the Access-Request which it sends to the AAA to validate the *MIP RRQ*. For cases where the MIP NAI from the triggering *MIP RRQ* does match a pre-existing binding and the HA needs to contact the AAA to validate the *MIP RRQ*, the HA shall include device session information about the old binding (e.g. WiMAX-Session-Id, any known CUI value) in the Access-Request which it sends to the AAA to validate the *MIP RRQ*.

#### 4.8.2.1.5.1 HA Requirements - Initial AAA-Request

Upon receiving RRQ for a MS for which there is no mobility binding exists, the HA SHALL send a RADIUS Access-Request or Diameter WHA4R command as per [37] to fetch the MN-HA key needed to authenticate the MIP RRQ. If needed, the HA also requests for the HA-RK key to validate the corresponding authentication extension. The HA always send the RADIUS Access-Request packet or Diameter WHA4R command to the local AAA server. If the HA is in visited network, the RADIUS Access-Request or Diameter WHA4R command is sent to the VAAA.

The HA SHALL include the contents of the NAI Extension received in the MIP4 RRQ in the User-Name attribute, and the MN-HA-MIP4-SPI. In the case of RADIUS, the HA SHALL include the Message-Authenticator (80) attribute used to integrity protect the RADIUS Access-Request packet. The value of the Message-Authenticator attribute is set in accordance with the computation specified in [40] for RADIUS Access-Request packet.

The HA SHALL either set the NAS-IP to the IPv4 address of the HA facing the AAA server, or set the NAS-IPv6 to the IPv6 address of the HA facing the AAA server, or both (The IP address of the NAS Client running on the HA).

The HA-IP address SHALL be set to the value of the HA-IP address facing the FA in the hHA-IP-MIP4 attribute.

If FA-HA key is required, the HA SHALL include HA-RK-SPI indicating it needs the HA-RK key. The HA-RK-SPI value should be set to the same FA-HA SPI value received from MIP RRQ.

The HA SHALL set its WiMAX-Capability in the WiMAX-Capability attribute.

The HA SHALL include the CUI attribute set to NULL if it requires the HAAA to include the CUI of the user in the RADIUS Access-Accept or Diameter WHA4A command.

Note: For binding different pseudo-IDs, the CUI could be used. If not present, use another attribute, e.g., last-pseudonym.

#### **4.8.2.1.5.2 HA Requirements - Processing Initial AAA Response**

The AAA server's role is to transport the correct keys back to the HA. The AAA server does not authenticate the Mobile IP Registration Request. The AAA server MAY however return a RADIUS Access-Reject or in the case of Diameter, failure result code of Diameter WHA4A command if it cannot find the user session state cached during Device/User Authentication and Authorization procedures, or if there were other errors.

In the case of RADIUS, upon receiving an RADIUS Access-Accept packet (see 4.3.5) in response to its RADIUS Access-Request packet the HA SHALL verify the Message-Authenticator (80) attribute using the procedures defined in [40]. If the Message-Authenticator is not valid, the HA SHALL silently discard the RADIUS Access-Accept packet.

The RADIUS Access-Accept or Diameter WHA4A command contains an MN-HA key that the HA uses to validate the MN-HA AE. If the HA requested the HA-RK key by including the HA-RK-SPI in the RADIUS Access-Request or Diameter WHA4R AND/OR WHA6R command, then the local AAA server will include the HA-RK key in the RADIUS Access-Accept packet or Diameter WHA4A command.

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 AE if optional FA-HA AE is used.

If the CUI attribute is include and the HA supports CUI then the HA SHALL include the received CUI in all Accounting packets exchanged with the Home-AAA. See [74].

If the HA receives Prepaid attributes and the HA supports Prepaid, the HA SHALL provide the prepaid processing as specified in section 4.4.3.3.

If the HA receives Hot-lining attributes and the HA supports Hot-lining, the HA SHALL support Hot-lining as specified in section 4.4.3.5.

Upon successful processing of the RADIUS Access-Accept packet or Diameter WHA4A command, if the HA has advertised Accounting support in the Access-Request/WHA4R and the WiMAX-Capability in the Access-Accept/WHA4A message, then the HA SHALL generate a RADIUS Accounting-Request or Diameter ACR command (Start) message for that the Mobile IPv4 session.

#### **4.8.2.1.5.3 HA Processes AAA-Reject**

If the HA receives a RADIUS Access-Reject packet or failure result code of Diameter WHA4A command in response to its RADIUS Access-Request or Diameter WHA4R command, and the Registration Request includes an invalid MN-HA authentication extension the HA SHALL reject the mobile node's registration and should perform one of the following:

- If there is a valid FA-HA authentication extension or an alternative security association, then the home agent SHALL send a Registration Reply with Code 131.
- In all other cases, the home agent MAY send a Registration Reply to the mobile node with Code 131.

In either case, the HA SHALL discard the Request.

#### **4.8.2.1.5.4 HA Processing MIP4 Registration Request Indicating Termination**

When the HA receives a MIP4 Registration Request with lifetime = 0, the HA SHALL validate the MN-HA AE included in the RRQ. If the validation is successful, the HA SHALL remove the mobility binding for the NAI (user) and it SHALL generate a RADIUS Accounting-Request or Diameter ACA command (Stop) packet if it is configured to do accounting for the MIP4 session. The HA SHALL respond back with an RRP (w/ lifetime=0) to confirm the successful de-registration. If the MN-HA AE validation fails, the HA SHALL silently discard the RRQ

and it MAY log the event for help in system administration. In this case, the HA SHALL not remove the mobility binding of the user (NAI).

#### 4.8.2.1.6 AAA Server Requirements

If the HA is located in the visited network, the VAAA will receive RADIUS Access-Request packet or Diameter WHA4R command from the HA during Mobile IP procedures. The following text describes the Mobile IPv4 procedure for VAAA server.

The VAAA server acts as a RADIUS/Diameter proxy transporting RADIUS packets/Diameter messages between the visited HA and the HAAA.

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

During proxy operation the VAAA Proxy SHALL validate Message-Authenticator in all RADIUS packets. If the RADIUS packets received are invalid, the VAAA proxy SHALL discard the RADIUS packets.

During routing operations the VAAA SHALL process the NAI found in the User-Name attribute as specified by [68] and route the AAA messages accordingly. If VAAA chooses to send the AAA messages following the same route as taken by the network access authentication AAA messages, it MAY decorate the NAI with the decoration remembered from the network access authentication procedure.

If the visited HA has requested HA-RK by including the HA-RK-SPI in the RADIUS Access-Request or Diameter WHA4R command, the VAAA SHALL include HA-RK-KEY and HA-RK-Lifetime attributes corresponding to the HA-RK-SPI in the RADIUS Access-Accept or Diameter WHA4A command to be forwarded to the HA. The values of HA-RK-KEY and HA-RK-Lifetime are locally cached on the VAAA server per Authenticator, and the same values are returned to the Authenticator during access authentication.

The HAAA server receives RADIUS Access-Request packet or Diameter WHA4R command from the HA if the HA is located in the home network, or from the VAAA if the HA is located in the visited network during Mobile IP procedures. The following text describes the Mobile IPv4 procedures for HAAA server.

Upon receiving the RADIUS Access-Request packets that contains Message-Authenticator (80) attribute, the RADIUS server SHALL validate the value of the Message-Authenticator (80) as described in [40]. If the authenticator fails to validate, the RADIUS server SHALL silently discard the RADIUS Access-Request. A RADIUS Access-Request which does not contain a Message-Authenticator (80) SHALL be silently discarded.

The User-Name attribute contains the PMIP-Authenticated-Network-Identity or the Outer-Identity of the user established during Device/User Network Access Authentication and Authorization. The HAAA SHALL use this identity to fetch the MIP session context for this user session.

With respect to Mobile IP, the session context contains:

- True identity of the user;
- HoA that MAY have been assigned to the user;
- MIP Key context (keys, SPIs, lifetimes).

If the HAAA is unable to fetch the session context then this indicates that the user has not been previously authenticated and the HAAA SHALL reply back with an RADIUS Access-Reject or failure result code of Diameter WHA4A command to the HA.

If the device session information (e.g. WiMAX-Session-Id, CUI) in the HA -> AAA Access-Request does not match the latest value device session information known by the AAA for the associated MIP Id, the AAA shall recognize that the received device session information is stale but shall not consider this a reason to generate an Access-Reject. If the AAA ultimately decides to generate an AAA->HA Access-Accept (e.g. based on SPI, MIP ID match), the AAA shall include the latest device session information (e.g. WiMAX-Session-Id, CUI if requested by HA) known for the referenced MIP\_Id along with any other settings (e.g. filters etc) that apply to the new binding.

The HAAA SHALL obtain the MN-HA key computed using the HA-IP address from the MIP key context, associated with the value of MN-HA SPI included in MN-HA Authentication Extension. If the SPI in the received request is not associated with MN-HA key in the MIP key context, the HAAA SHALL reply back with an RADIUS



Access-Reject or failure result code of Diameter WHA4A command to the HA. If the HA is in visited network, the HAAA SHALL additionally check the HA-IP address is the same HA address provided by VAAA during access authentication. If there is a mismatch, the HAAA SHALL reply back with an RADIUS Access-Reject or failure result code of Diameter WHA4A command to the VAAA.

If the HA is in the home network and it requested the HA-RK key by including the HA-RK-SPI, then the HAAA SHALL include HA-RK-KEY and hHA-RK-Lifetime attributes corresponding to the hHA-RK-SPI. The values of HA-RK-KEY and HA-RK-Lifetime are locally cached on the HAAA server per Authenticator, and the same values are returned to the Authenticator during access authentication.

The HAAA server MAY need to include other attributes in the response back to the HA as follows:

- If the MS is a prepaid subscriber and the HA supports the Prepaid Client (as indicated in the WiMAX-Capability attribute received in the RADIUS Access-Accept packet or Diameter WHA4A command. If the policy is to use the HA for prepaid, then the AAA server SHALL include the prepaid attributes in the RADIUS Access-Accept (see section PREPAID) or Diameter WHA4A command.
- If the MS is to be hot-lined, as indicated by the user-profile, then if the HA supports Hot-lining capability as specified by the WiMAX-Capability attribute received in the RADIUS Access-Request or Diameter WHA4R command, then if the policy specifies to use the HA as the hot-lining device, the AAA server SHALL include the hot-lining attributes in the RADIUS Access-Accept (see section HOT-LINING) or Diameter WHA4A command.
- If the RADIUS Access-Request or Diameter WHA4R command included the CUI attribute set to null, then the AAA server SHALL compute a value for the CUI (see section CUI) and set the CUI attribute to this value.
- Prior to sending the RADIUS Access-Accept packet the HAAA MAY (per local policies) sign the RADIUS Access-Accept packet using the Message-Authenticator(80) attribute as specified in [40].

The HAAA server SHALL receive RADIUS Access-Request packets or Diameter AAR with Diameter Network Access Server Application from the DHCP server as per RFC4005 [62], during the DHCP authentication sub-option procedure, when the DHCP server needs a DHCP-RK that corresponds to the DHCP-RK-ID received in the DHCPDISCOVER message.

The following text describes the DHCP-RK delivery procedure.

In the case of RADIUS, upon receiving the RADIUS Access-Request packets that contains a Message-Authenticator (80) attribute, the AAA server SHALL validate the value of the Message-Authenticator (80) as described in [40]. If the authenticator fails to validate, the AAA server SHALL silently discard the RADIUS Access-Request. An RADIUS Access-Request, which does not contain a Message-Authenticator (80), SHALL be silently discarded.

The AAA server SHALL retrieve the DHCP-RK-Key-ID and if the key identifier is not known to the AAA server, the AAA server SHALL respond with the RADIUS Access-Reject message or a WiMAX DHCP Request command with Result-Code indicating an error.

If the DHCP-RK is successfully retrieved, the AAA server SHALL send the retrieved key to the DHCP server in an RADIUS Access-Accept packet or WiMAX DHCP Request command described by the following text.

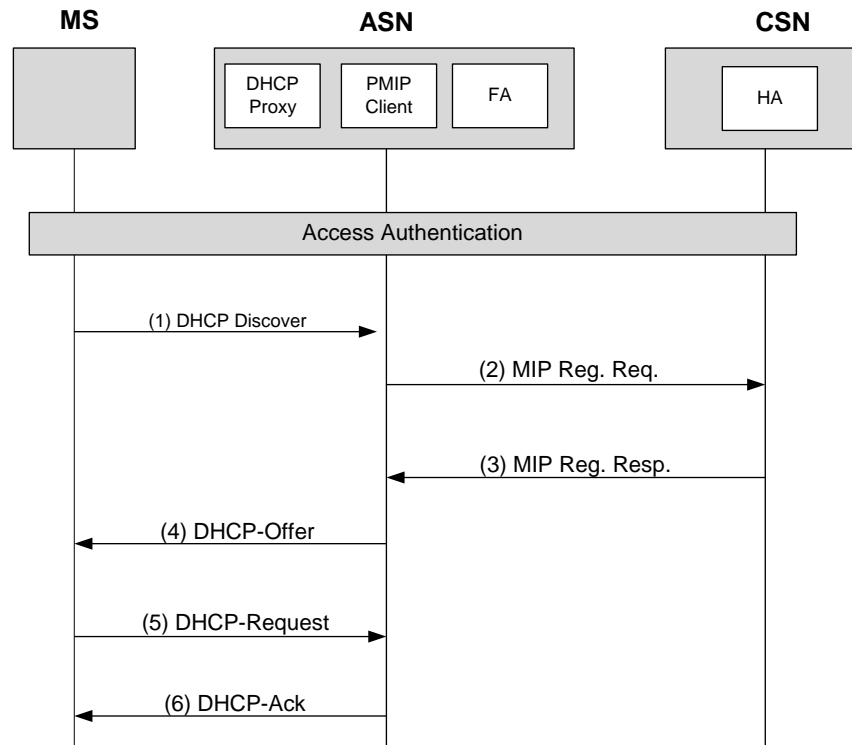
In case of RADIUS, the AAA server SHALL include the Message-Authenticator (80) attribute used to integrity protect the RADIUS Access-Accept packet. The value of the Message-Authenticator attribute is set in accordance with the computation specified in [40].

The AAA server SHALL include the following attributes:

- DHCP-RK;
- The DHCP-RK-Key-ID associated with the DHCP-RK-KEY and the DHCP server;
- The DHCP-RK-Lifetime.

#### 4.8.2.1.7 PMIP4 Connection Setup Call Flow

##### 4.8.2.1.7.1 DHCP Proxy in ASN



**Figure 4-122 – PMIP4 Connection Setup Procedure**

The NAS receives HA address and PMIP4 security context from the HAAA at the time of successful Device/User Access Authentication. NAS may also receive HoA address if it is assigned by HAAA. Subsequently, the following steps happen.

#### STEP 1

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

#### STEP 2

Upon receiving the DHCPDISCOVER message, the DHCP Proxy triggers the PMIP4 client to initiate the Mobile IPv4 Registration procedure. If HoA (HAAA assigns HoA) was received during access authentication, then the PMIP4 client uses the HoA information and constructs a Mobile IPv4 Registration Request message. If HoA was not access authentication received, then the HoA field is set to 0.0.0.0. In either case, the CoA field is set to the FA-CoA address that is configured locally. PMIP4 client sends the Mobile IPv4 Registration Request to the FA address. The FA forwards the registration request to the HA. The source address for this Mobile IPv4 message over R3 is FA-CoA, and the destination address is HA address.

#### STEP 3

If an HoA is 0.0.0.0 in the Mobile IP Registration Request message, the HA assigns an HoA. Otherwise, the HoA in the Mobile IP Registration Request message is used. The HA responds with the Mobile IP Registration Response message. The source address for this Mobile IPv4 message over R3 is HA, and the destination address is FA-CoA. The FA forwards the message to the PMIP4 client.

**STEP 4**

The PMIP4 client passes this information to the DHCP proxy. The DHCP proxy sends the DHCPOFFER message to the MS. A minimal number of DHCPOFFER messages should be sent, preferably only one.

**STEP 5**

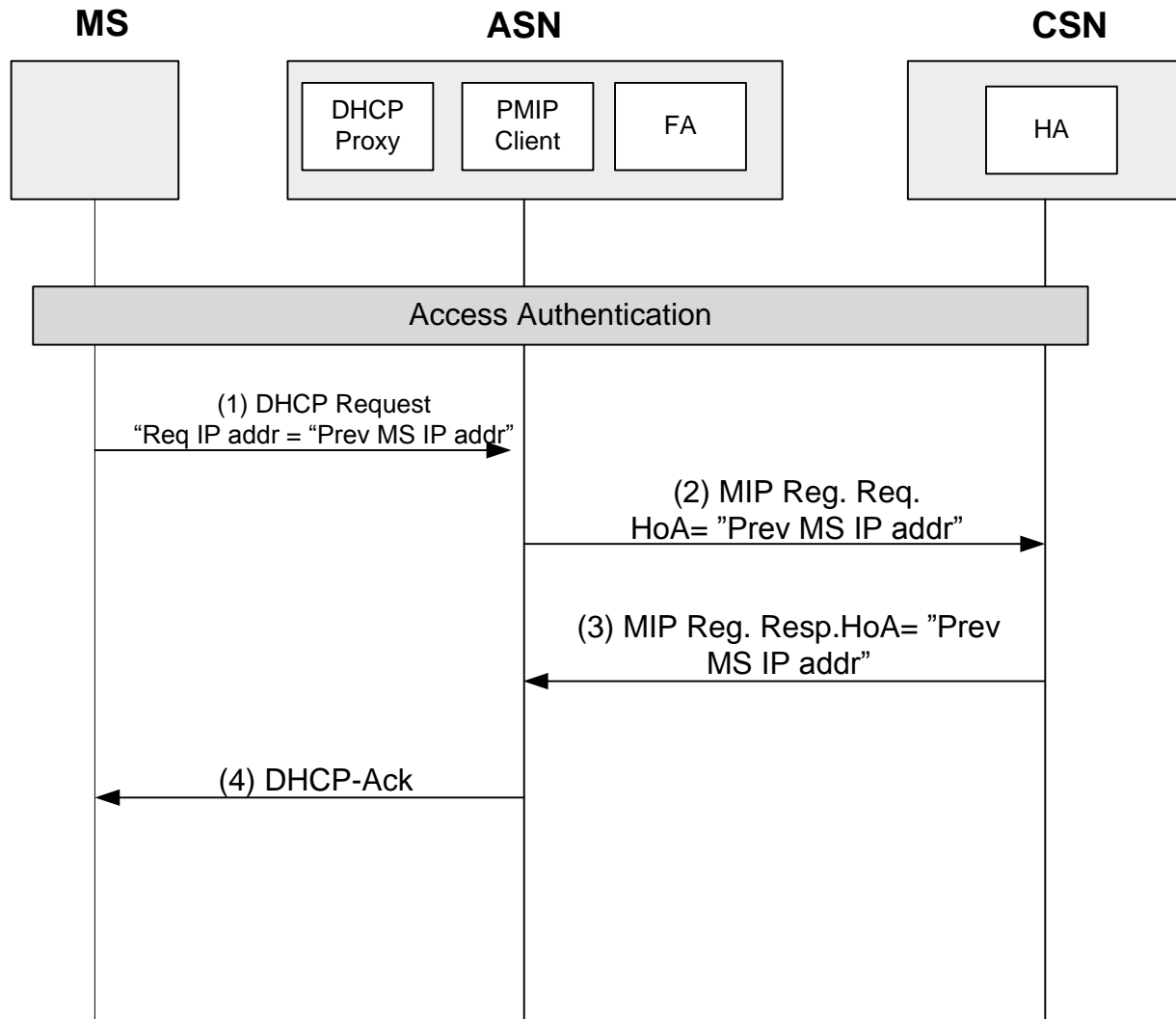
MS responds to the first DHCPOFFER message received with a DHCPREQUEST to the DHCP Proxy with the information received in the DHCPOFFER.

**STEP 6**

The DHCP Proxy acknowledges the use of this IP address and other configuration parameters as defined in [24] by sending the DHCPACK message.

**4.8.2.1.7.2 DHCP Proxy in ASN - DHCP Request message specifies the MS previously assigned IP address**

In this scenario, after performing successful network entry EAP authentication, the DHCP client in MS is trying to obtain the same IP address e.g., the DHCP lease timer from a previous network entry has not expired. The MS, in this case, uses the DHCP Request message to indicate the requested IP address.



**Figure 4-123– DHCP Session Renewal in PMIP4 case via DHCP Request - DHCP Proxy in ASN**

### STEP 1

The MS sends a DHCP Request to the DHCP Proxy collocated with Anchor DPF/FA GW in order to renew its IP address.

If the requested IP address is released or the IP address is assigned to another MS, DHCP Proxy SHALL send DHCPNAK to the MS, the DHCP Client will behave as specified in [24]. And MIP Registration procedure (STEP 2 - 4) SHALL be skipped.

### STEP 2 - 3

Upon receiving the DHCP REQUEST from the MS, The DHCP Proxy/PMIP client sends the MIP RRQ message to the HA with home address field set to the requested IP address. If HA maintains the binding record for the given MS, it returns the HoA address in the MIP Registration Response to the Anchor ASN.

If the HA doesn't maintain the binding record for the given MS or can't assign the requested HoA to the MS, the HA SHALL reject the MIP Registration Request by sending MIP Registration Reply with Code set to 129- 'administratively prohibited'. Upon receiving the MIP rejection from HA, the Proxy DHCP/PMIP Client consequently sends a DHCPNAK to the MS and skips step 4.

#### STEP 4

The Anchor ASN SHALL process the DHCP Request message and reply with a DHCP Ack to MS.

In case of the MIP failure, the DHCP Proxy/PMIP Client SHALL send DHCPNAK message to MS. Then the DHCP Client will behave as specified in [24].

##### 4.8.2.1.7.2.1 DHCP Proxy in ASN Timers and Timer Considerations

All timers are set and cleared according to DHCP ([24]) and MIP ([48]) specifications.

##### 4.8.2.1.7.3 DHCP Relay in ASN

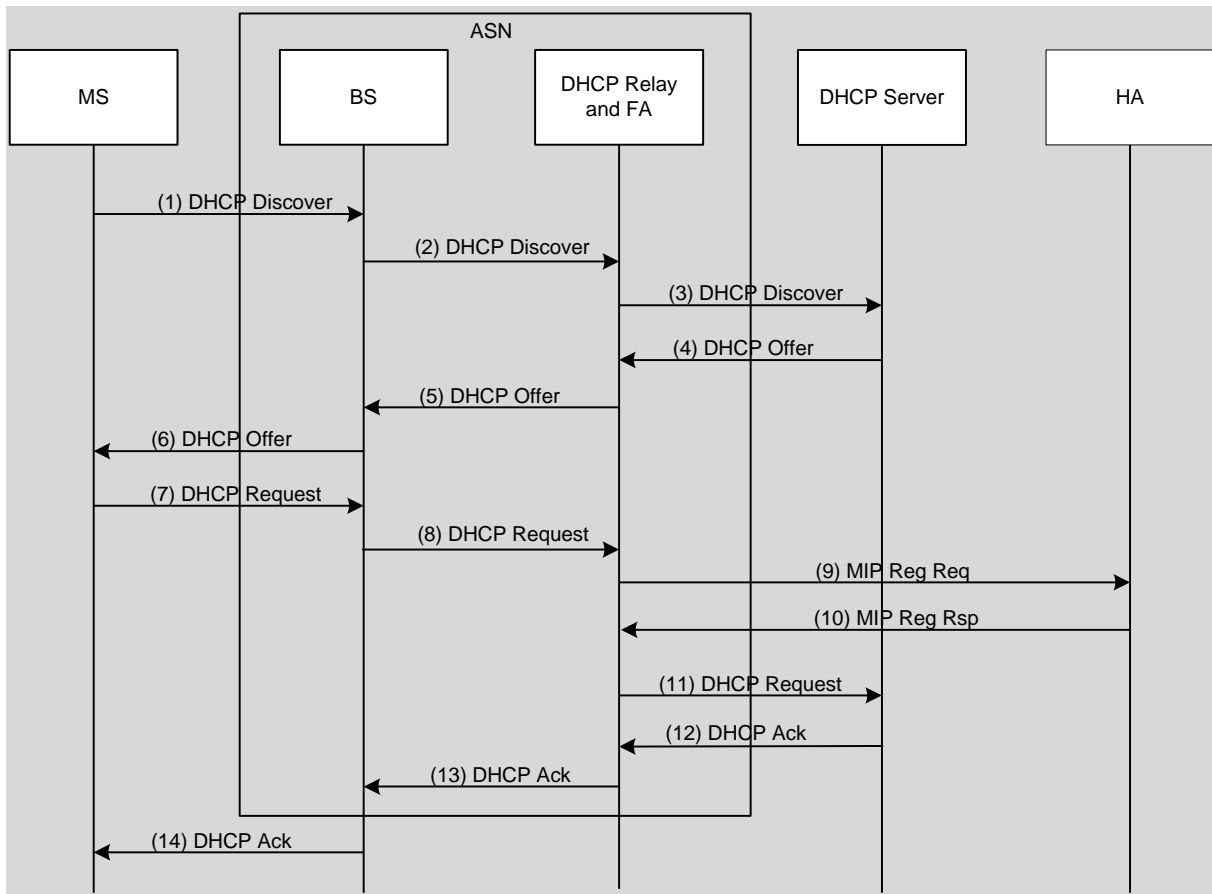


Figure 4-124 – PMIP4 Connection Setup - DHCP Relay in ASN

The following steps are written based on R3 is already secured. If R3 is not secured, the DHCP Relay SHALL add the authentication sub-option as explained in [65] to have data integrity and replay protection for relayed DHCP messages.

#### STEP 1

The MS sends a DHCP Discover as a broadcast message. The DHCP message is sent on the MS's Initial service flow setup over R1 interface to the BS.

#### STEP 2

The DHCP Discover message is forwarded from BS to DHCP Relay present in ASN through the data path established for the ISF (Initial Service Flow) traffic.

**STEP 3**

The DHCP Relay in ASN will intercept and change the destination IP address from broadcast to unicast and configure the giaddr field in the DHCP payload and sends the DHCP Discover message to the DHCP server of the MS based on configuration information. The configuration information in the most generic case will be downloaded via AAA but it may also be statically provisioned.

The DHCP relay MAY send a unicast DHCP Discover message to each DHCP server listed in the Access-Accept message.

If the Datapath is per MS or per SF, the MS context can be found based on the Datapath and not on the MAC address. If the Datapath is per BS the MS context can be found based on the MAC address or MS NAI.

**STEP 4**

DHCP servers receiving the DHCP Discover request reply by sending a DHCP Offer message including an offered IP address.

**STEP 5**

The DHCP Relay in ASN forwards the DHCP replies to the MS. The DHCP Offer message is sent from ASN GW to BS through the Data Path.

The destination IP address of the DHCP Offer message sent to MS is a unicast one. Normally DHCP servers or relay agents attempt to deliver the DHCP Offer to a MS directly using unicast delivery. Unfortunately some MS's implementations are unable to receive such unicast IP datagram until they know their own IP addresses. To work around with this kind of MSs, broadcast address MAY be used in DHCP Offer message. ASN need to check the BROADCAST (B) flag in the DHCP Offer message. If this flag is set, ASN need use broadcast address to send DHCP Offer message, otherwise unicast address, but the delivery will be over a unicast CID. If there are multiple DHCP Offer messages, DHCP Relay forwards each received message to the MS.

**STEP 6**

BS sends DHCP Offer message to the MS on the MS's Initial Service Flow.

**STEP 7**

MS receives one or more DHCP Offer message, and sends a DHCP Request to the selected DHCP server as a broadcast message confirming its choice of the DHCP Server.

**STEP 8**

DHCP Request message is sent from BS to DHCP relay in ASN through the Data Path established.

**STEP 9**

The DHCP Relay in the ASN prompts the PMIP client to initiate the Mobile IP Registration procedure. The PMIP client uses the HoA information to construct a Mobile IP Registration Request message. This message contains HoA and CoA for this MS. The source address for this R3 message is CoA, and the destination address is HA address.

**STEP 10**

The HA responds with the Mobile IP Registration Response message in which the source address for this R3 message is HA address, and the destination address is CoA.

**STEP 11**

After the establishment of MIP tunnel the PMIP client informs the DHCP Relay about the MIP registration result. The DHCP Relay in ASN relays the DHCP Request with the optional MIP registration result encapsulated in the WiMAX vendor specific relay agent suboption as defined in section 4.8.2.1.2.2 to the DHCP server.

**STEP 12**

The selected DHCP server receives the DHCP Request and replies with a DHCP Ack containing the configuration information requested by the MS.

**STEP 13**

The DHCP Relay relays the DHCP Ack to the BS.

**STEP 14**

BS sends DHCP Ack message to the MS on the MS's provisioned Initial Service Flow.

If MS doesn't receive a DHCP Ack, or DHCP Nak message when timeout, it will retransmit DHCP Request. If neither DHCP Ack nor DHCP Nak received when the maximum retransmission reached, MS SHALL restart the IP initialization process.

**4.8.2.1.7.3.1 DHCP Relay in ASN Error Conditions**

**4.8.2.1.7.3.1.1 Timers and Timer Considerations**

All timers are set and cleared according to DHCP ([24]) and MIP ([48]) specifications.

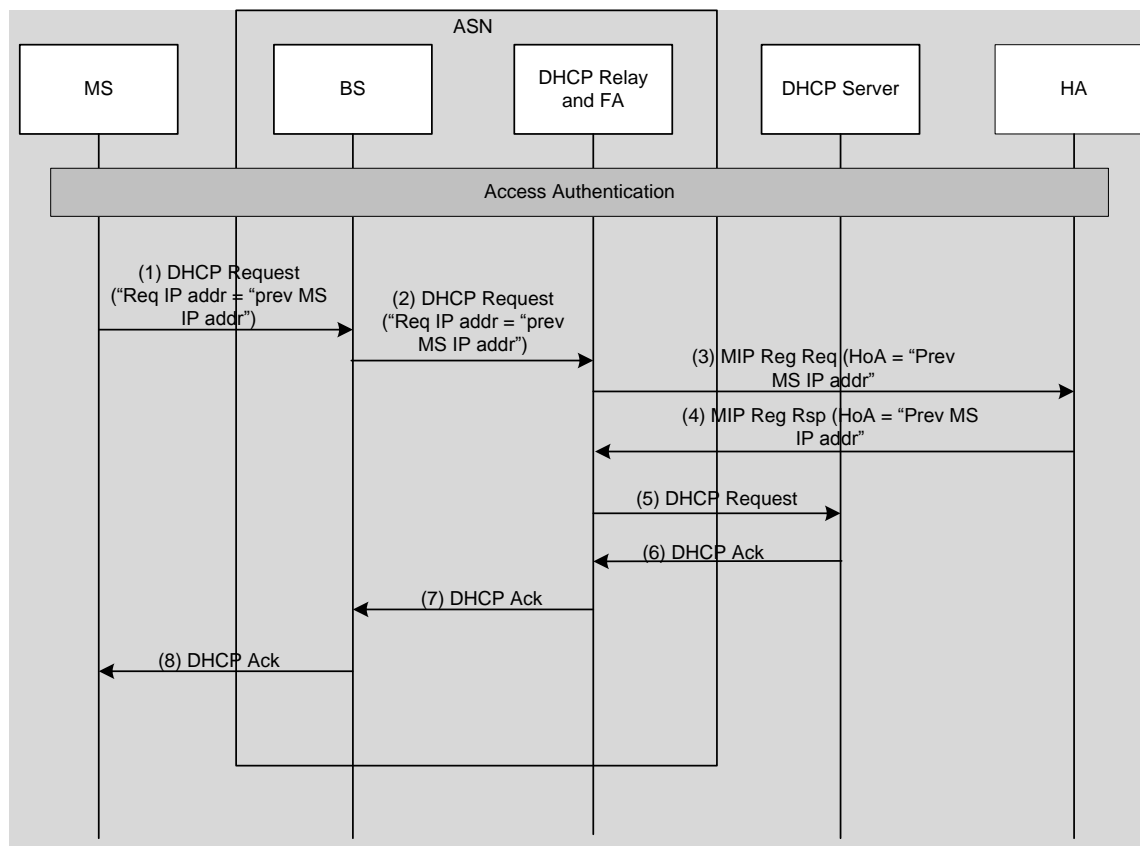
**4.8.2.1.7.3.1.2 Proxy MIP Registration Error Considerations**

The DHCP Server confirms the PoA address allocation to this MS upon receipt of the DHCP Request. If the MIP registration result is not successful, as indicated by the WiMAX vendor specific relay agent suboption that includes MIP registration result failure code, the DHCP Server responds DHCP NAK echoing the WiMAX vendor specific relay agent suboption and releases the reserved address. If this suboption is not sent to the DHCP server and the MIP registration indicates a failure, the DHCP relay SHALL NOT forward the DHCPREQUEST message to the DHCP server (thus causing DHCP offer to expire) and the network SHALL perform an exit for the corresponding MS.

**4.8.2.1.7.3.1.3 DHCP PoA Address Allocation Error Considerations**

If the MIP registration succeeded before and the PoA address assignment failed, the DHCP relay triggers the PMIP4 client to initiate MIP4 deregistration procedures.

#### 4.8.2.1.7.4 DHCP Relay in ASN - DHCP Request message specifies the MS previously assigned IP address



**Figure 4-125 - DHCP Session Renewal in PMIP4 case via DHCP Request - DHCP Relay in ASN**

In this scenario, after performing successful network entry EAP authentication, the MS is trying to obtain the same IP address because the DHCP lease timer from a previous network entry has not expired. The MS, in this case, uses the DHCP Request message to indicate the requested IP address

##### STEP 1

The MS sends a DHCP Request to the BS in order to renew its IP address, Required IP address field is set to MS previous IP address.

##### STEP 2

DHCP Request message is sent from BS to DHCP relay in ASN through the Data Path established.

##### STEP 3

Upon receiving the DHCP REQUEST from the MS, the DHCP Relay/PMIP Client sends the MIP RRQ message to the HA with home address field set to the requested IP address. The source address for this MIP RRQ message is CoA, and the destination address is HA address.

##### STEP 4

If HA assigns the same HoA address to the MS it SHALL return the HoA address in the MIP Registration Response to the Anchor ASN. If the HA cannot assign the requested HoA to the MS, the HA SHALL reject the MIP Registration Request by sending MIP Registration Reply with Code set to 129- 'administratively prohibited'.



1 The HA IP address policy and assignment is outside the scope of this specification.

2 **STEP 5**

3 After the establishment of MIP tunnel the PMIP client informs the DHCP Relay with the MIP registration result.  
4 The DHCP Relay in ASN relays the DHCP Request with the optional MIP registration result encapsulated in the  
5 WiMAX vendor specific relay agent suboption as defined in section 4.8.2.1.2.2 to the DHCP server.

6 The DHCP relay MAY send a unicast DHCP Request message to each DHCP server listed in the Access-Accept  
7 message.

8 If DHCP Server receives MIP rejection in vendor specific relay agent suboption, the DHCP Server consequently  
9 sends DHCP NAK to the MS.

10 **STEP 6**

11 The DHCP server receives the DHCP Request and replies with a DHCP Ack containing the configuration  
12 information requested by the MS.

13 **STEP 7**

14 The DHCP Relay relays the DHCP Ack to the BS.

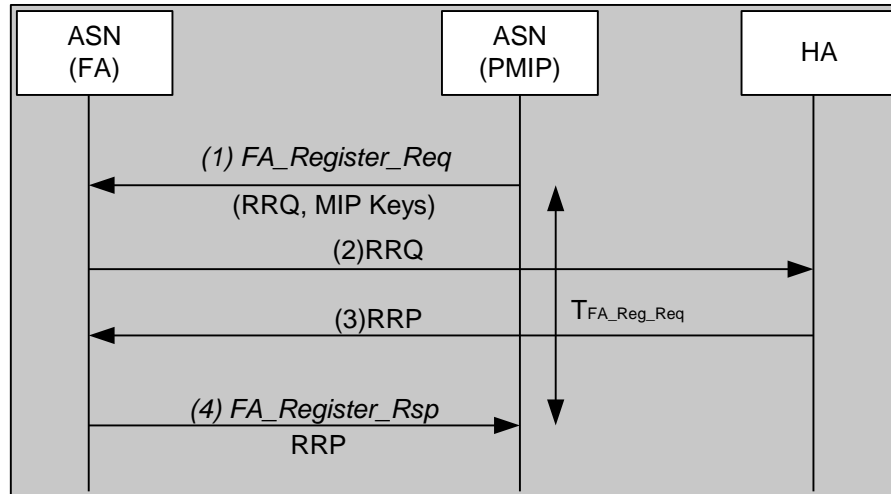
15 **STEP 8**

16 BS sends DHCP Ack message to the MS on the MS's provisioned Initial Service Flow.

17 If MS doesn't receive a DHCP Ack, or DHCP Nak message when timeout, it will retransmit DHCP Request as  
18 specified in [24]. If neither DHCP Ack nor DHCP Nak received when the maximum retransmission reached, the  
19 DHCP Client in MS will behave as specified in [24].

20 **4.8.2.2 Proxy MIP4 Session Renewal Procedure**

21 The PMIP4 Client SHALL refresh the MIP4 binding with the FA and the HA on behalf of the MS. This procedure is  
22 transparent to the MS since the DHCP RENEW and REBIND states are not tied to the Mobile IPv4 Registration  
23 Lifetime (which the MS is unaware of). Figure 4-126 shows steps involved in Proxy MIP4 Session Renewal  
24 procedure.



**Figure 4-126 – PMIP4 Session Renewal Procedure**

#### STEP 1

The PMIP4 client initiates the MIP registration with the FA by sending *FA\_Register\_Req* message. The FA information is obtained from the PMIP4 Context available at the PMIP4 client. This message contains a fully formed RRQ according to RFC3344, with CoA field in the RRQ set to the CoA of the FA. The source address of the RRQ is that of the MS and the destination address is the CoA or the FA address if FA address is different from CoA. In addition, *FA\_Register\_Req* message contains the FA-HA MIP key if this key is used. A timer  $T_{FA\_Reg\_Req}^{15}$  is started for *FA\_Register\_Rsp* from ASNb.

#### STEP 2

After receiving *FA\_Register\_Req*, the ASN (where the FA resides) FA relays the RRQ to the HA.

#### STEP 3

The HA responds with the RRP.

#### STEP 4

The ASN (where the FA resides) relays the MIP RRP encapsulated in an *FA\_Register\_Rsp* message to the PMIP4 client. The PMIP4 client updates the FA information in its record and stops  $T_{FA\_Reg\_Req}$ .

#### 4.8.2.2.1 MS Requirements

The MS SHALL support the DHCP client function as defined in [25]. The address renewal by the MS SHALL be based on the T1 (RENEW) and T2 (REBIND) timers as defined in the RFC.

#### 4.8.2.2.2 DHCP Requirements

##### 4.8.2.2.2.1 DHCP Proxy

The DHCP proxy SHALL implement the DHCP lease renewal process as per [25]. When the DHCP proxy receives a DHCPREQUEST message from the MS for an IPv4 address for which the Lease Time is either close to T1 or T2 value, it SHALL respond back to the MS with DHCPACK message. Note that, PMIP4 client performs MIP binding renewal automatically and if it fails, it will update DHCP proxy (refer to section 4.8.2.2.3).

Since all DHCP proxies in the NAP are assigned with the same IP address, the DHCP message sent by the MS will be terminated by the DHCP proxy collocated with anchor DPF/FA.

<sup>15</sup> The value of  $T_{FA\_Reg\_Req}$  and retransmission behavior should be per RFC3344.

#### 4.8.2.2.2.2 DHCP Relay in ASN

The anchor data path ASN GW SHALL act as a DHCP relay and SHALL intercept every DHCP message originated by the MS. The DHCP relay SHALL perform the verification of the 'chaddr' field in the DHCP message and other security related checks as described in 4.8.2.1.7.3.1. DHCP relay SHALL relay the DHCP message to the DHCP server in the CSN, in accordance with the [44]. If R3 is not secured (e.g., by IPsec), the DHCP relay SHALL authenticate relayed DHCP messages by providing the relay agent authentication suboption ([65]).

#### 4.8.2.2.3 PMIP4 Client Requirements

The PMIP4 Client SHALL perform the same procedures as defined in section 4.8.2.1.3 to renew the MIP4 binding with the HA when PMIP4client and FA are collocated in the same ASN. Otherwise, PMIP4client SHALL use FA\_Register\_Req and FA\_Register\_Rsp messages for MIP registration over R4 as shown in steps 4 to 7 of PMIP4 CSN MM Handover procedure in section 4.8.2.3.7.1.

#### 4.8.2.2.4 FA Requirements

The FA requirements are the same as section 4.8.2.1.4.

#### 4.8.2.2.5 HA Requirements

The HA SHALL process the RRQ for binding renewal for an existing binding cache entry the same way as defined in section 4.8.2.1.5.

#### 4.8.2.2.6 AAA Server Requirements

Same as section 4.8.2.1.6.

#### 4.8.2.2.7 PMIP4 Session Renewal Call Flows

##### 4.8.2.2.7.1 DHCP Session Renewal Flows

##### 4.8.2.2.7.1.1 DHCP Proxy

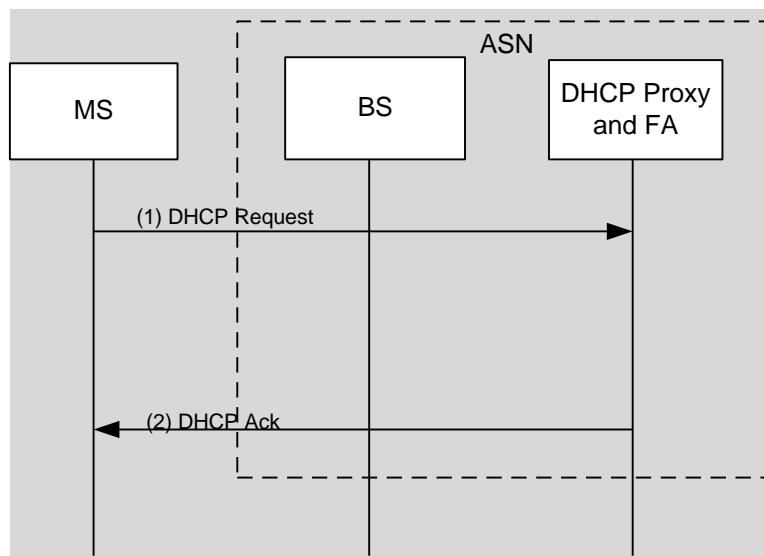


Figure 4-127 – DHCP Session Renewal in PMIP4 case- DHCP Proxy in ASN

#### STEP 1

The MS sends a DHCP Request to the DHCP Proxy collocated with Anchor DPF/FA GW in order to renew its IP address.

## STEP 2

The Anchor ASN SHALL process the unicast DHCP Request message and reply with a DHCP Ack to MS.

In case of DHCPNAK message, the PMIP4 client may initiate the MIP deregistration procedure, if DHCP Proxy and PMIP4 client are not collocated the DHCP Proxy may send FA\_Revoke\_Req to trigger PMIP4 client or alternatively the MS MAY initiate network exit. If the MS does not receive any response from the DHCP Proxy, the MS does number of retries and then MAY initiate network exit.

### 4.8.2.2.7.1.2 DHCP Relay in ASN

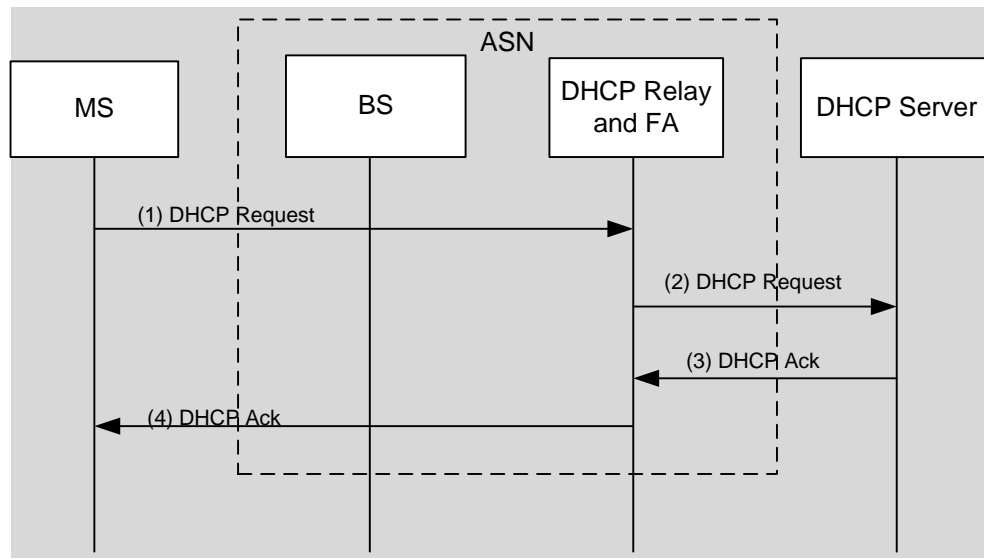


Figure 4-128 – DHCP Session Renewal in PMIP4 case- DHCP Relay in ASN

## STEP 1

The MS sends a DHCP Request to the DHCP server in order to renew its IP address.

## STEP 2

The Anchor ASN MAY monitor the unicast DHCP Request message and forwards it to the DHCP server.

## STEP 3

The DHCP server replies with a DHCP Ack to ASN.

## STEP 4

The DHCP relay forwards the DHCP ACK message to MS. In case of DHCP NAK message, the PMIP4 client may initiate the MIP deregistration procedure, if DHCP relay and PMIP4 client are not collocated the DHCP relay may send FA\_Revoke\_Req to trigger PMIP4 client or alternatively the MS may initiate Network exit. If the MS does not receive any response from the DHCP server the MS does number of retries and then MAY initiate Network exit.

### 4.8.2.2.7.1.2.1 DHCP Relay in ASN Timers and Timer Considerations

All timers are set and cleared according to DHCP ([24]) and MIP ([48]) specifications.

### 4.8.2.2.7.2 MIP4 Session Renewal Flows

Same as the PMIP4 session establishment procedure described in section 4.8.2.1.

#### 4.8.2.3 Proxy MIP4 CSN Anchored Mobility Handover

The detailed call flows for the PMIP4 based CSN Anchored Mobility is described in section 4.8.2.3.7. This section describes CSN anchored mobility handover without re-authentication.

If the FA relocation is due to MS moving from one FA to another FA, before the FA relocation, the ASN anchored mobility events occur, and its detail procedure is shown in section 4.7. In order to prevent packet loss and reduce handoff latency, the temporary R4 data path between two ASNs MAY be established.

The relocation of the FA SHALL always be negotiated between the Anchor ASN and the Serving ASN. Both the Anchor ASN and the Serving ASN can initiate the negotiation. If the Anchor ASN initiates the negotiation, it SHALL send an Anchor DPF HO\_Req message with its own CoA address, DHCP context information for the MS and other layer3 context maintained by the Anchor to the Serving ASN. This message SHALL be addressed to the DPF in Serving ASN, whose address is known since it is on the data path to the MS. If the Serving ASN agrees to take over the FA functionality after this negotiation, then it SHALL send an Anchor\_DPF\_Relocate\_Req message to the PMIP4 client using the information provided by the Anchor ASN. If for any reason the Serving ASN rejects FA relocation, then further action of Serving/Anchor ASN is implementation specific.

If the Serving ASN initiates the negotiation, it SHALL send an Anchor DPF HO Trigger message to the anchor DPF in Anchor ASN, and the Anchor ASN starts the source initiated negotiation as indicated above. In both cases, only after both Anchor ASN and the Serving ASN agree with the Anchor relocation, the Serving ASN will send an *Anchor\_DPF\_Relocate\_Req* to the PMIP4 client to start MIP registration procedure.

**Table 4-113 – Anchor\_DPF\_HO\_Req Message**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>Authenticator ID	5.3.2.19	M	
>DHCP Relay Info	5.3.2.56	O	Information about the DHCP Relay. Anchor ASN SHALL include this TLV if operating in PMIP4 DHCP Relay mode.
>>DHCP Server Address	5.3.2.57	O	The IP address of the DHCP Server.
>>DHCP Relay Address	5.3.2.55	O	DHCP Relay IP address for which the key is requested.
>>DHCP Key	5.3.2.51	O	Key used to calculate and authenticate messages between the DHCP relay and DHCP server.
>>DHCP Key ID	5.3.2.52	O	Key ID associated with the key used to compute authentication suboption.
>>DHCP Key Lifetime	5.3.2.53	O	The remaining lifetime in seconds of the DHCP key.
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	The TLV contains one or more packet classification rules.
>>>Classification Rule Index	5.3.2.30	CM	This TLV SHALL be included if Packet Classification Rule / Media Flow Description is included in the transmitted message.
>>>Classification Rule Priority	5.3.2.32	O	The value of the field specifies the priority for the

IE	Reference	M/O	Notes
			Classification Rule.
>>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	The values of the field specify the matching parameters for the IP type of service/DSCP byte range and mask.
>>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...
>>>>IP Source Address and Mask	5.3.2.84	O	An IP source address and its corresponding address mask.
>>>>IP Destination Address and Mask	5.3.2.82	O	An IP destination address and its corresponding address mask.
>>>>Protocol Source Port Range	5.3.2.140	O	The value of the field specifies a range of protocol Source port values.
>>>>Protocol Destination Port Range	5.3.2.139	O	The value of the field specifies a range of protocol destination port values.
>>>>Associated PHSI	5.3.2.15	O	The Associated PHSI value.
>Anchor MM Context	5.3.2.11	M	DHCP Proxy Info, DHCP Server List, MIP4 Info, etc.
>>MIP4 Info	5.3.2.96	M	MIP4 Info.
>>MS Mobility Mode	5.3.2.104	M	This TLV SHALL be set to indicate PMIP4.
>>DHCP Proxy Info	5.3.2.54	O	Anchor ASN SHALL include this TLV when operating in PMIP4 Proxy DHCP mode.
>>>>IP Remained Time	5.3.2.83	O	Remaining lease time for the assigned IP address. This TLV SHALL be included if DHCP Proxy Info is included in the transmitted message.
>>>>DNS IP Address	5.3.2.374	O	The IPv4/IPv6 address of the DNS server.  One or more instances of this TLV may be present depending on the number of DNS addresses delivered by the AAA server. When more than one address is present, the first TLV SHALL be the primary DNS server and the remaining are secondary DNS servers.
>>Idle Mode Info	5.3.2.80	O	
>>HA IP Address	5.3.2.75	O	
>>Home Address (HoA)	5.3.2.77	O	
>>Care-of Address (CoA)	5.3.2.28	M	
>PPAQ	5.3.2.131	O	Used during PPA Relocation. This TLV (both expended and the original Quota) SHALL be included if online accounting is activated in the Serving ASN.
>>Quota Identifier	5.3.2.148	CM	This TLV SHALL be included if PPAQ is included in the transmitted message.

IE	Reference	M/O	Notes
>>Volume Quota	5.3.2.167	O	
>>Volume Threshold	5.3.2.168	O	
>>Volume Used	5.3.2.357	O	
>>Duration Quota	5.3.2.275	O	
>>Duration Threshold	5.3.2.276	O	
>> Duration Used	5.3.2.132	O	
>>Resource Quota	5.3.2.277	O	
>>Resource Threshold	5.3.2.278	O	
>>Update Reason	5.3.2.279	O	
>>Service-ID	5.3.2.280	O	
>>Rating-Group-ID	5.3.2.281	O	
>>Termination Action	5.3.2.282	O	
>>Pool-ID	5.3.2.283	O	
>>Pool-Multiplier	5.3.2.284	O	
>>Prepaid Server	5.3.2.285	O	This TLV SHOULD be included if available (provided by HAAA).
>>SFID (one or more)	5.3.2.184	O	SF ID(s) SHALL be included in flow based prepaid accounting scenario.
> MS Authorization Context	5.3.2.100	O	
>> MS NAI	5.3.2.105	CM	
>> R3 WiMAX Capability	5.3.2.207	CM	
>>> R3 WiMAX-Release	5.3.2.441	CM	This TLV SHALL be included if R3 WiMAX Capability is included in the transmitted message.
>>> R3 Accounting Capabilities	5.3.2.208	CM	This TLV SHALL be included if R3 WiMAX Capability is included in the transmitted message.
>>> R3 Hotlining Capability	5.3.2.408	O	This TLV SHALL be Present as a part of HLD Relocation; when HLD is Collocated in FA.
>> R3 WiMAX Session ID	5.3.2.214	CM	
>> R3 Packet Flow Descriptor	5.3.2.215	CM	
>>> SFID	5.3.2.184	CM	
>>> R3 Packet Data Flow ID	5.3.2.216	CM	
PPAC	5.3.2.65	O	Describes the Prepaid Capabilities of the ASN. This TLV SHALL be included if online accounting is activated in the Serving ASN for the particular MS session. If Target ASN does not support any of the required online accounting capabilities, it SHOULD reject Anchor DPF relocation procedure.

IE	Reference	M/O	Notes
>AvailableInClient	5.3.2.89	CM	This TLV SHALL be included if PPAC is included in the transmitted message.
Hotlining Context	5.3.2.400	O	This TLV SHALL be Present as a part of HLD Relocation; when HLD is Collocated in FA.
> R3 IP-Redirection-Rule	5.3.2.403	O	
> R3 NAS-Filter-Rule	5.3.2.404	O	
> R3 HTTP-Redirection-Rule	5.3.2.402	O	
> Remaining Hotline Session Timer	5.3.2.406	O	
> R3 Hotline-Indication	5.3.2.407	O	
> Service-Id	5.3.2.280	O	

1

**Table 4-114 – Anchor\_DPF\_HO\_Trigger Message**

IE	Reference	M/O	Notes
PPAC	5.3.2.65	O	Describes the Prepaid Capabilities of the ASN. This TLV SHALL be included if online accounting is activated in the Serving ASN for the particular MS session. If Target ASN does not support any of the required online accounting capabilities, it SHOULD reject Anchor DPF relocation procedure.
>AvailableInClient	5.3.2.89	CM	This TLV SHALL be included if PPAC is included in the transmitted message.
Accounting Context	5.3.2.204	O	
>Accounting Mode Provisioning	5.3.2.243	CM	This TLV SHALL be included if the Accounting Context TLV is included in the transmitted message.
>>Accounting Type	5.3.2.247	CM	This TLV SHALL be included if the Accounting Mode Provisioning TLV is included in the transmitted message.
MS Info	5.3.2.103	O	
> MS Authorization Context	5.3.2.100	O	
>> MS NAI	5.3.2.105	CM	
>> R3 WiMAX Capability	5.3.2.207	CM	
>>> R3 WiMAX-Release	5.3.2.441	CM	
>>> R3 Accounting Capabilities	5.3.2.208	CM	
>>> R3 Hotlining Capability	5.3.2.408	O	This TLV SHALL be Present as a part of HLD Relocation; when HLD is Collocated in FA.
>> R3 WiMAX Session ID	5.3.2.214	CM	



IE	Reference	M/O	Notes
>> R3 Packet Flow Descriptor	5.3.2.215	CM	
>>> SFID	5.3.2.184	CM	
>>> R3 Packet Data Flow ID	5.3.2.216	CM	

The mobility event MAY not require relocation of the PMIP4 Client and the Authenticator, for that case, only the FA SHALL be relocated to a target ASN. During the FA relocation, DHCP context along with other Layer3 context maintained by the Anchor ASN for the MS SHALL be transferred to the target ASN. The PMIP4 Client SHALL initiate a MIP4 registration on behalf of the MS via the target FA.

After the MIP registration, the Serving ASN will take over the FA role and it SHALL send an Anchor DPF *HO\_Rsp* message to the previous Anchor ASN. Upon receiving the Anchor DPF *HO\_Rsp* message with success indication, the previous Anchor ASN SHALL remove the mobility binding, the DHCP context information and the R4 data path.

**Table 4-115 – Anchor\_DPF\_HO\_Rsp Message**

IE	Reference	M/O	Notes
Result Code	5.3.2.154	M	Success or failure indication.

After the CSN anchored handover is successfully completed, the target FA SHALL send the Context\_Rpt message to the serving BS. The Context\_Rpt message must contain the address of the new anchor DPF function. Upon receipt of the Context\_Rpt message containing the address of the new anchor DPF, the serving BS must update its notion of the location of the anchor DPF function for this MS. The serving BS SHALL confirm the receipt of the Context\_Rpt message by sending the Context\_Ack message.

**Table 4-116– Context\_Rpt from Target FA to Serving BS**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Set to indicate “MS Network Context” (bit #1).
MS Info	5.3.2.103	M	
>Anchor ASN GW ID	5.3.2.154	M	Identifies the target ASN-GW in relocation.

**Table 4-117– Context\_Ack from Serving BS to Target FA**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Identifies the target ASN-GW in relocation.

#### 4.8.2.3.1 MS Requirements

There are no specific MS requirements for CSN anchored mobility management with PMIP4.

#### 4.8.2.3.2 DHCP Proxy/Relay Requirements

##### 4.8.2.3.2.1 DHCP Proxy in ASN

The DHCP proxy, collocated with the Anchor DPF/FA SHALL be relocated to the target ASN if the R3 mobility event occurs. The DHCP Proxy Info should be transmitted during relocation.

The old Anchor ASN SHALL remove the DHCP context information for the MS, once it receives a success indication from the Target ASN that FA has been relocated.

#### 4.8.2.3.2 DHCP Relay in ASN

The DHCP relay, collocated with the Anchor DPF/FA SHALL be relocated to the target ASN if the R3 mobility event occurs. The DHCP Relay Info should be transmitted during relocation.

After the successful R3 relocation event, the new anchor data path ASN GW SHALL act as a DHCP relay for the MS. In the course of the R3 relocation, the address of the DHCP server is transferred as part of the MS context from the serving to the target ASN GW.

The new anchor data path ASN GW SHALL intercept every DHCP message originated by the MS. It SHALL perform the verification of the ‘chaddr’ field in the intercepted DHCP message and other security related checks as described in 4.8.2.1.2.2. DHCP relay SHALL relay the intercepted DHCP message to the DHCP server in the CSN, in accordance with the [44]. If R3 is not secured (e.g., by IPsec), the DHCP relay SHALL authenticate relayed DHCP messages by providing the relay agent authentication suboption ([65]).

#### 4.8.2.3.3 PMIP4 Client Requirements

Upon receiving an *Anchor\_DPF\_Relocate\_Req* from the Serving ASN, and the Source FA-CoA matching the FA Identity on its record, the PMIP4 Client SHALL send a *FA\_Register\_Req* message to the Serving ASN to initiate a MIP4 registration on behalf of the MS via the target FA. If the Source FA-CoA does not match the FA identity on its record, the PMIP4 Client SHALL send an *Anchor\_DPF\_Relocate\_Rsp* message to the Serving ASN with Result Code set to Failure.

**Table 4-118 – Anchor\_DPF\_Relocate\_Req Message**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>Anchor MM Context	5.3.2.11	M	
>>MS Mobility Mode	5.3.2.104	M	
>>MIP4 Info	5.3.2.96	M	
>>>Target FA IP Address	5.3.2.70	O	This TLV is included if the Target Care-of Address is not the same as the target FA.
>>>Target Care-of Address	0	M	Care-of Address for the Target FA
>>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA) of the Serving FA.

**Table 4-119 – FA\_Register\_Req Message**

IE	Reference	M/O	Notes
RRQ	5.3.2.20	M	Defined in MIP RFC.
MIP4 Security Info	5.3.2.266	O	
>PMIP-Authenticated-Network-Identity	5.3.2.41	O	Include when assigned by AAA in the Access-Accept. Indicates the authorized PMIP NAI for use by PMIP Client.
>FA-HA Key	5.3.2.66	O	FA-HA if used.
>FA-HA Key Lifetime	5.3.2.67	O	

IE	Reference	M/O	Notes
>FA-HA SPI	5.3.2.68	O	

**Table 4-120 – FA\_Register\_Rsp Message**

IE	Reference	M/O	Notes
RRP	5.3.2.97	M	Defined in MIP RFC.

**Table 4-121 – Anchor\_DPF\_Relocate\_Rsp Message**

IE	Reference	M/O	Notes
Result Code	5.3.2.154	M	Failure indication. The Anchor_DPF_Relocate_Rsp is sent only in the case of Failure.

#### 4.8.2.3.4 FA Requirements

In general the requirements specified in 4.8.2.1.4 SHALL apply to the FA.

#### 4.8.2.3.5 HA Requirements

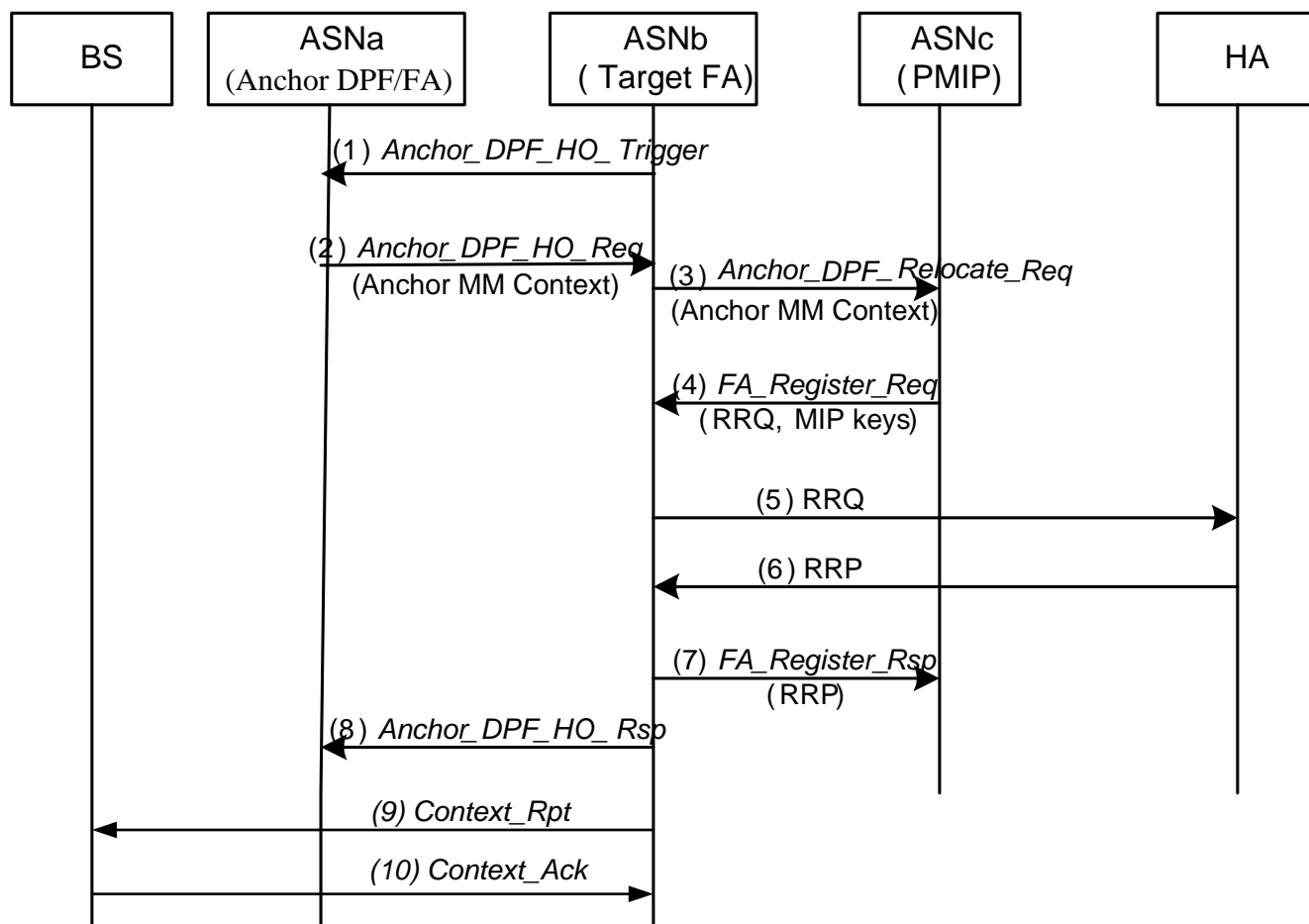
The HA SHALL process the RRQ the same way as defined in 4.8.2.1.5. The HA SHALL modify the binding cache entry for the MS to reflect the new CoA (of the target FA). After processing the RRQ successfully, the HA SHALL begin to forward packets destined for the MS to the new CoA. The HA MAY send Revocation message to the previous FA to terminate binding.

#### 4.8.2.3.6 AAA Server Requirements

There are no specific AAA Server requirements for CSN anchored mobility management with PMIP4.

### 1 4.8.2.3.7 PMIP4 Mobility Procedure

#### 2 4.8.2.3.7.1 PMIP4 CSN MM Handover



**Figure 4-129 – CSN-Anchored Mobility (PMIP)**

#### 6 STEP 1

7 If the target ASNb initiates the FA relocation negotiation (Pull Mode), it sends an *Anchor\_DPF\_HO\_Trigger*  
8 message to the anchor DPF in ASNa. If ASNa agrees with the FA relocation, it proceeds to Step 2. After sending  
9 *Anchor\_DPF\_HO\_Trigger*, ASNb starts a timer  $T_{\text{Anchor\_DPF\_HO\_Trigger}}$  for *Anchor\_DPF\_HO\_Req*. Once  
10 *Anchor\_DPF\_HO\_Req*, indicating the FA relocation decision of ASNa, is received by ASNb,  $T_{\text{Anchor\_DPF\_HO\_Trigger}}$  is  
11 stopped.

12 If the source ASNa initiates the FA relocation procedure (Push Mode), the call flow starts from Step 2.

#### 13 STEP 2

14 ASNa sends an *Anchor\_DPF\_HO\_Req* message to the DPF in ASNb. The message contains the DHCP context  
15 information for the MS and the Authenticator Id (Authenticator is co-located with the PMIP client) which is used to  
16 locate the PMIP client, and ASNa will start a timer  $T_{\text{Anchor\_DPF\_HO\_Req}}$ <sup>16</sup> for *Anchor\_DPF\_HO\_Rsp* from ASNb.

<sup>16</sup>  $T_{\text{Anchor\_DPF\_HO\_Req}}$  value should be larger than the sum of  $T_{\text{AnchorDPF\_Relocate\_Request}}$  and  $T_{\text{FA\_Register\_Request}}$  including retransmission

The *Anchor\_DPF\_HO\_Trigger*(ASNb) and *Anchor\_DPF\_HO\_Req*(ASNa) may be triggered independently. If the ASNa receives *Anchor\_DPF\_HO\_Trigger* after sending the *Anchor\_DPF\_HO\_Req* between steps 2 and 8, ASNa ignores the *Anchor\_DPF\_HO\_Trigger* message. Otherwise, the ASNa sends the *Anchor\_DPF\_HO\_Req* to the ASNb.

### STEP 3

If the Target ASN (ASNb) does not accept FA relocation it proceeds directly to Step 8.

The ASNb sends an *Anchor\_DPF\_Relocate\_Req* message to the PMIP4 client, and starts a timer  $T_{\text{Anchor\_DPF\_Relocate\_Req}}$  for *FA\_Register\_Req*. This message relays information about target ASN that is necessary in order to construct and send the MIP RRQ message in step 4. The message contains CoA for the target FA, and target FA address if it is different from the CoA. In addition to target FA-CoA, source FA-CoA is included in the message for the validation.

### STEP 4

The PMIP4 client verifies that the source 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 [48], 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 is the target CoA or the FA if the target FA address is different from the target CoA. In addition, *FA\_Register\_Req* message contains the FA-HA MIP key if this key is used. This message is sent to the Target ASN, whose address was identified as the source address of the *Anchor\_DPF\_Relocate\_Req* message in step 3. A timer  $T_{\text{FA\_Reg\_Req}}$ <sup>17</sup> is started for *FA\_Register\_Rsp* from ASNb.

### STEP 5

After receiving *FA\_Register\_Req*, ASNb stops  $T_{\text{Anchor\_DPF\_Relocate\_Req}}$ . 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  $T_{\text{FA\_Reg\_Req}}$ . Upon receipt of the *FA\_Register\_Rsp* at the PMIP Client, the PMIP4 Context at the PMIP Client is updated with the new Registration Lifetime.

### 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  $T_{\text{Anchor\_DPF\_HO\_Req}}$  started in step 2. Either ASNa or ASNb initiate Path Deregistration procedure [4.12.4]. Note, that in order to minimize impact on the user traffic, Data Path between ASNa and ASNb may be preserved for a while (time interval is implementation specific), to ensure delivery of the late user packets through ASNa.

If the Target ASN does not accept FA relocation it responds with an *Anchor\_DPF\_HO\_Rsp* message with Result Code set to Failure. ASNa also stops  $T_{\text{Anchor\_DPF\_HO\_Req}}$  started in step 2.

### STEP 9

ASNb sends Context Report to the BS. The *Context\_Rpt* message contains the address of the new anchor DPF function.

---

<sup>17</sup> The value of  $T_{\text{FA\_Reg\_Req}}$  and retransmission behavior should be per [48].

## STEP 10

BS updates location of the anchor DPF function for this MS upon receipt of the Context\_Rpt message. The BS confirms the receipt of the Context\_Rpt message by sending the Context\_Ack message.

### 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.

- $T_{\text{Anchor\_DPF\_HO\_Trigger}}$ : is started by target ASNb upon sending an *Anchor\_DPF\_HO\_Trigger* message. It is stopped upon receiving a corresponding *Anchor\_DPF\_HO\_Req*.
- $T_{\text{Anchor\_DPF\_HO\_Req}}$ : is started when serving ASNa sends an *Anchor\_DPF\_HO\_Req* and is stopped upon receiving a corresponding *Anchor\_DPF\_HO\_Rsp*.
- $T_{\text{Anchor\_DPF\_Relocate\_Req}}$ : 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*.
- $T_{\text{FA\_Reg\_Req}}$ : 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 4-122 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-122 – Timer Values for PMIP4 CSN MM Handover Messages over R4/R3**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{\text{Anchor\_DPF\_HO\_Trigger}}$	TBD		TBD
$T_{\text{Anchor\_DPF\_HO\_Req}}$	TBD		TBD
$T_{\text{Anchor\_DPF\_Relocate\_Req}}$	TBD		TBD
$T_{\text{FA\_Reg\_Req}}$	TBD		TBD

### 4.8.2.3.7.1.2 PMIP4 CSN MM Handover Error Conditions

This section describes error conditions associated with the PMIP4 CSN MM Handover procedure.

#### 4.8.2.3.7.1.2.1 Timer Expiry

Table 4-123 shows details on the corresponding actions associated with timer expiry. 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 5-70B Timer Expiry Conditions.

**Table 4-123 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{\text{Anchor\_DPF\_HO\_Trigger}}$	Target FA	PMIP4 CSN MM handover is aborted and further action of Serving/Target FA is implementation Specific.
$T_{\text{Anchor\_DPF\_HO\_Req}}$	Serving FA	PMIP4 CSN MM handover is aborted and further action of Serving/Target FA is implementation Specific.
$T_{\text{Anchor\_DPF\_Relocate\_Req}}$	Target FA	PMIP4 CSN MM handover is aborted and

		<i>Anchor_DPF_HO_Rsp</i> is sent to ASNa with Result Code set to Failure.
T_FA_Register_Req	PMIP4 client	PMIP4 CSNMM Handover is aborted.

#### 4.8.2.3.7.1.2.2 Current FA-CoA Mismatches the FA on PMIP4 client

*Anchor\_DPF\_Relocate\_Rsp* with Result Code set to Failure is sent to the sender of *Anchor\_DPF\_Relocate\_Req*. And PMIP4 CSN MM Handover is aborted. This message will also trigger *Anchor\_DPF\_HO\_Rsp* with a failure indication.

#### 4.8.2.3.7.1.2.3 MIP Registration Failure

It can be caused due to many reasons, such as authentication failure. In this case, PMIP4 CSN MM handover is aborted and *Anchor\_DPF\_HO\_Rsp* is sent to ASNa with Result Code set to Failure and further action of Serving/Target FA is implementation specific.

#### 4.8.2.4 Proxy MIP4 Session Termination

There are various reasons for termination of an ongoing session for a user. The termination MAY be due to:

- The MS sending a DHCPRELEASE message;
- The IP address lease timer expires at the DHCP proxy/DHCP Relay or FA initiated session release;
- Authenticator initiated release due to re-authentication timeout or AAA initiated release;
- HA decides to release session of the MS and send Registration Revocation message to the FA (Refer to [50]).

For PMIP4 session termination triggered network exit, see section 4.5.1.2.4.

##### 4.8.2.4.1 MS Requirements

When the MS needs to terminate the IP session, it SHOULD send a DHCPRELEASE message to the DHCP proxy to gracefully terminate the L3 connection and release the assigned IP address.

##### 4.8.2.4.2 DHCP Requirements

###### 4.8.2.4.2.1 DHCP Proxy

Upon receiving a DHCPRELEASE from the MS or upon expiry of the lease timer for the HoA, the DHCP proxy SHALL notify the PMIP4 Client to de-register the MIP4 session for the MS.

The DHCP proxy SHALL release the IPv4 address lease (HoA) and any associated state for the MS upon receiving a notification of successful MIP4 de-registration from the PMIP4 Client.

###### 4.8.2.4.2.2 DHCP Relay in ASN

Upon intercepting a DHCPRELEASE from the MS, in addition to relaying the DHCPRELEASE message to the DHCP server, the DHCP relay SHALL notify the PMIP4 Client to de-register the MIP4 session for the MS.

##### 4.8.2.4.3 PMIP4 Client Requirements

Upon receiving a *FA\_Revoke\_Req* message from the FA for reasons such as DHCP initiated release or FA/HA initiated release, the PMIP4 client SHALL clear the mobility binding and reply back with a *FA\_Revoke\_Rsp* message.

**Table 4-124 – FA\_Revoke\_Req**

IE	Reference	M/O	Notes
FA Revoke Reason	5.3.2.16	M	DHCP release, expiry, FA initiated release, HA initiated release.

**Table 4-125 – FA\_Revoke\_Rsp**

IE	Reference	M/O	Notes
Result Code	5.3.2.154	M	Result of Revoke, Success or failure indication.

#### 4.8.2.4.4 FA Requirements

There is no specific requirement on the FA for the termination process.

#### 4.8.2.4.5 HA Requirements

The HA SHALL process the RRQ with Lifetime=0 and release the mobility binding for the user (NAI).

If accounting is enabled at the HA, the HA supporting RADIUS protocol SHALL send an Accounting-Request (Stop) packet with Acct-Terminate-Action set to “Session-Timeout” or “User-Request” depending on whether or not the session was terminated due to session time out (e.g., MIP lifetime timer expiry) or due to user request. In the case of an HA supporting Diameter, the HA SHALL send a WSTR command indicating that the session has terminated. As well, if accounting is enabled, the HA SHALL send a WACR command terminating the accounting session.

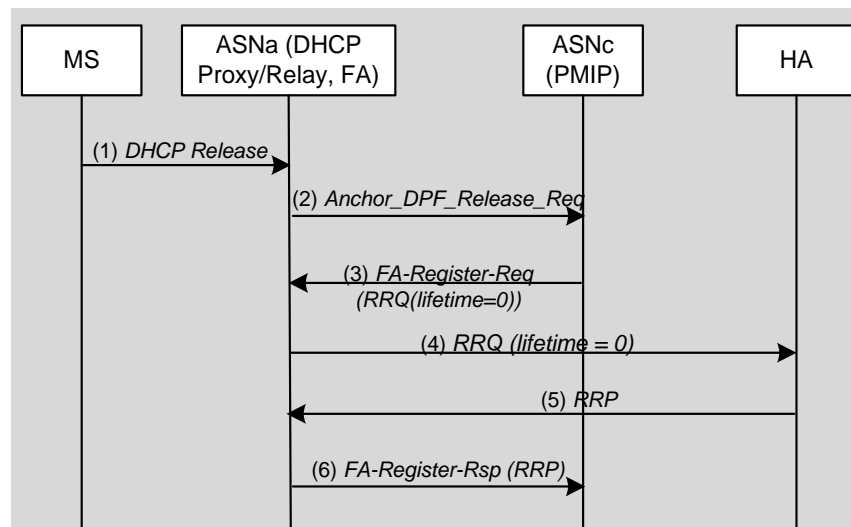
#### 4.8.2.4.6 AAA Server Requirements

Upon receiving the RADIUS Accounting-Request (Stop) message or Diameter WSTR command the AAA server SHALL signal the EAP server to delete all the keys and all other session information stored for this session.

#### 4.8.2.4.7 PMIP4 Session Release Procedure

##### 4.8.2.4.7.1 PMIP4 Session Release

##### 4.8.2.4.7.1.1 MS Initiated PMIP4 Session Release



**Figure 4-130 – PMIP4 Session Release Triggered by MS**

#### STEP 1

The trigger can be initiated by MS sending DHCP-Release message to the ASN(a) where the DHCP proxy/Relay and FA reside.



## STEP 2

The ASNa initiates the session release with PMIP4 client by sending *Anchor\_DPF\_Release\_Req* Message. At this point, ASNa starts a timer  $T_{Anchor\_DPF\_Release\_Req}$  to wait for *FA\_Register\_Req*.

## STEP 3

Upon receipt of *Anchor\_DPF\_Release\_Req* the ASNc sends *FA-Register-Req* (RRQ(lifetime=0)) to ASNa.

## STEP 4

Upon receipt of *FA-Register-Req* ASNa stops the timer  $T_{Anchor\_DPF\_Release\_Req}$ , extracts and relay the RRQ (lifetime = 0) to HA.

## STEP 5

The HA removes the binding and replies with RRP.

## STEP 6

After receiving RRP, ASN(a) sends *FA-Register-Rsp* (RRP) to the ASN(c).

Note: After IP session(s) is (are) released for an active MS, it is operator/network policy, when to trigger Network Exit for the MS as specified in section 4.5.2.

### 4.8.2.4.7.1.1.1 MS Initiated PMIP4 Session Release Timer and Timing Consideration

This section identifies the timer used during MS Initiated PMIP4 Session Release procedure.

- $T_{Anchor\_DPF\_Release\_Req}$ : is started by AnchorDPF ASNa, where DHCP proxy and FA are located, upon sending an *Anchor\_DPF\_Release\_Req* message. It is stopped upon receiving *FA-Register-Req* Message from the ASNc.

Table 4-126 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-126 – Timer Values for MS Initiated PMIP4 Session Release Messages over R4/R3**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{Anchor\_DPF\_Release\_Req}$	TBD		TBD

### 4.8.2.4.7.1.1.2 MS Initiated PMIP4 Session Release Error Conditions

This section describes error conditions associated with the MS Initiated PMIP4 Session Release procedure.

#### 4.8.2.4.7.1.1.2.1 Timer Expiry

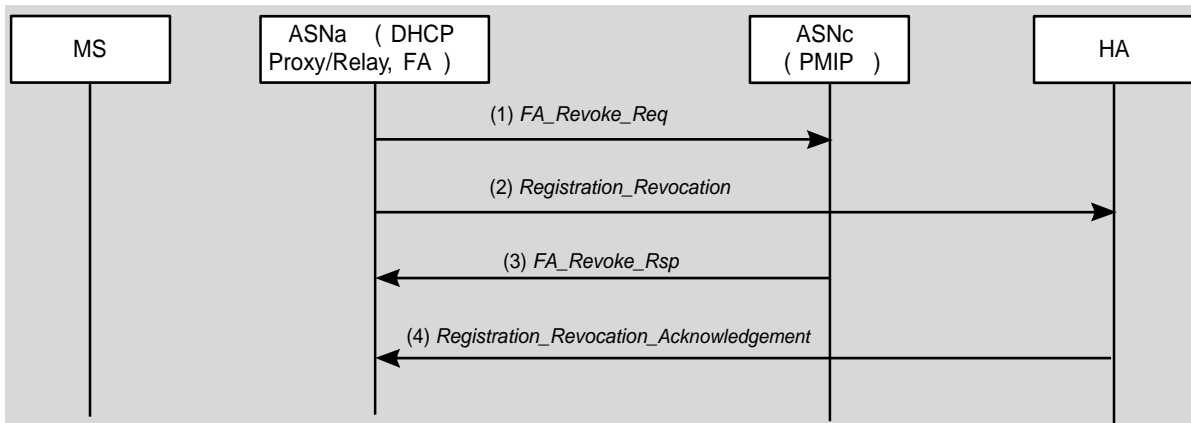
Table 4-127 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer expiry, if the maximum retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s) should be performed as indicated in Table 4-57.

**Table 4-127 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{Anchor\_DPF\_Release\_Req}$	AnchorDPF ASN	Behave as if <i>FA-Register-Req</i> is received. The Context information remained on PMIP4 and HA is

		released based on their time-out mechanism, which is implementation dependent.
--	--	--

#### 4.8.2.4.7.1.2 ASN Initiated PMIP4 Session Release



**Figure 4-131 – PMIP4 Session Release Triggered by ASN**

If RRQ which is the Default procedure used by ASN for PMIP4 session release then messages 2, 3, 4, 5 and 6 of section 4.8.2.4.7.1.1 will be used and follow the same procedures explained. Optionally Revocation can also be used for PMIP4 session release.

#### STEP 1, 2

The ASNa initiates the session release with PMIP4 client and HA concurrently by sending *FA\_Revoke\_Req* and *Registration Revocation* Message respectively. At this point, ASNa starts a timer  $T_{FA\_Revoke\_Req}$  to wait for *FA\_Revoke\_Rsp*<sup>18</sup>.

#### STEP 3, 4

*FA\_Revoke\_Rsp* and *Registration Revocation Acknowledgement* Message are received from PMIP4 client and HA respectively. After ASNa has received *FA\_Revoke\_Rsp* messages,  $T_{FA\_Revoke\_Req}$  is stopped.

#### 4.8.2.4.7.1.2.1 ASN Initiated PMIP4 Session Release Timer and Timing Consideration

This section identifies the timer used during ASN Initiated PMIP4 Session Release procedure.

$T_{FA\_Revoke\_Req}$ : is started by AnchorDPF ASNa, where DHCP proxy and FA are located, upon sending an *FA\_Revoke\_Req* message and a Registration Revocation message. It is stopped upon receiving both corresponding *FA\_Revoke\_Rsp* and Registration Revocation ACK message.

Table 4-128 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-128 – Timer Values for ASN Initiated PMIP4 Session Release Messages over R4/R3**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{FA\_Revoke\_Req}$	TBD		TBD

<sup>18</sup> The timer for Registration Revocation Message sent to the HA and retransmission behavior should be per [50].

#### 4.8.2.4.7.1.2.2 ASN Initiated PMIP4 Session Release Error Conditions

This section describes error conditions associated with the ASN Initiated PMIP4 Session Release procedure.

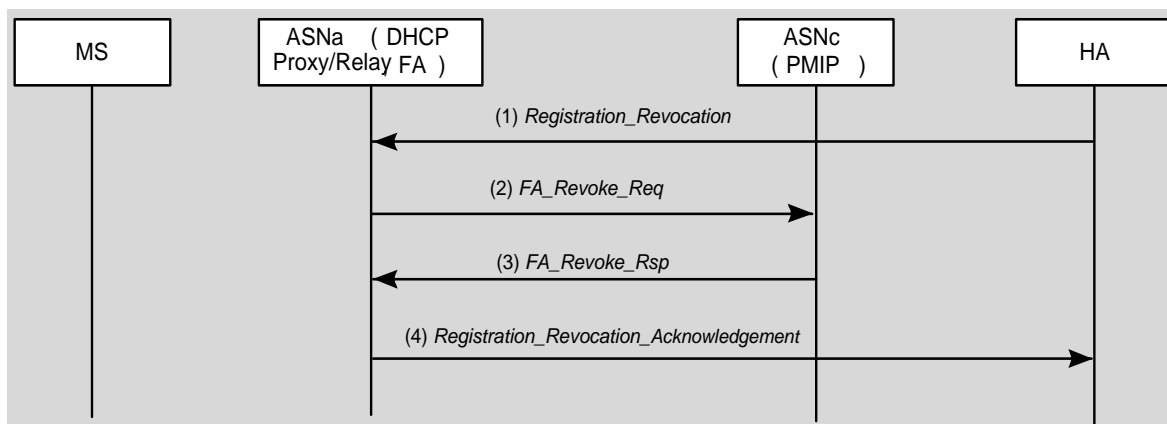
##### 4.8.2.4.7.1.2.2.1 Timer Expiry

Table 4-129 shows details on 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 4-49.

**Table 4-129 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T <sub>FA_Revoke_Req</sub>	AnchorDPF ASN	Behave as if both <i>FA_Revoke_Rsp</i> are received. The Context information remained on PMIP4 and HA is released based on their time-out mechanism, which is implementation dependent.

#### 4.8.2.4.7.1.3 HA Initiated PMIP4 Session Release



**Figure 4-132 – PMIP4 Session Release Triggered by HA**

##### STEP 1

The HA initiates the session release with FA by sending *Registration\_Revocation* Message. At this point, HA starts a timer T<sub>Registration\_Revocation</sub> to wait for *Registration\_Revocation\_Acknowledgement*<sup>19</sup>.

##### STEP 2

FA receiving *Registration\_Revocation* sends *FA\_Revoke\_Req* to PMIP4 client and starts T<sub>FA\_Revoke\_Req</sub> timer.

##### STEP 3

PMIP4 client upon receiving *FA\_Revoke\_Req* sends *FA\_Revoke\_Rsp* to FA.

<sup>19</sup> The timer for Registration Revocation Message sent by the HA and retransmission behavior should be per [50].

#### STEP 4

FA receiving *FA\_Revoke\_Rsp* stops the timer  $T_{FA\_Revoke\_Req}$ , deletes the PMIP context of the MS and sends *Registration\_Revocation\_Acknowledgement* to HA. HA on receiving *Registration\_Revocation\_Acknowledgement* message stops  $T_{Registration\_Revocation}$  timer.

##### 4.8.2.4.7.1.3.1 HA Initiated PMIP4 Session Release Timer and Timing Consideration

This section identifies the timer used during HA Initiated PMIP4 Session Release procedure.

- $T_{Registration\_Revocation}$ : is started by HA, upon sending a *Registration\_Revocation* message. It is stopped upon receiving *Registration\_Revocation\_Acknowledgement*.

Table 4-130 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-130 – Timer Values for HA Initiated PMIP4 Session Release Messages**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{Registration\_Revocation}$	TBD		TBD

##### 4.8.2.4.7.1.3.2 HA Initiated PMIP4 Session Release Error Conditions

This section describes error conditions associated with the HA Initiated PMIP4 Session Release procedure.

##### 4.8.2.4.7.1.3.2.1 Timer Expiry

Table 4-131 shows details on 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 4-49.

**Table 4-131 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{Registration\_Revocation}$	HA	Behave as if <i>Registration_Acknowledgement</i> is received and release the MIP tunnel.

#### 4.8.2.4.7.1.4 R3 Session Release – Initiated by Authenticator or AAA

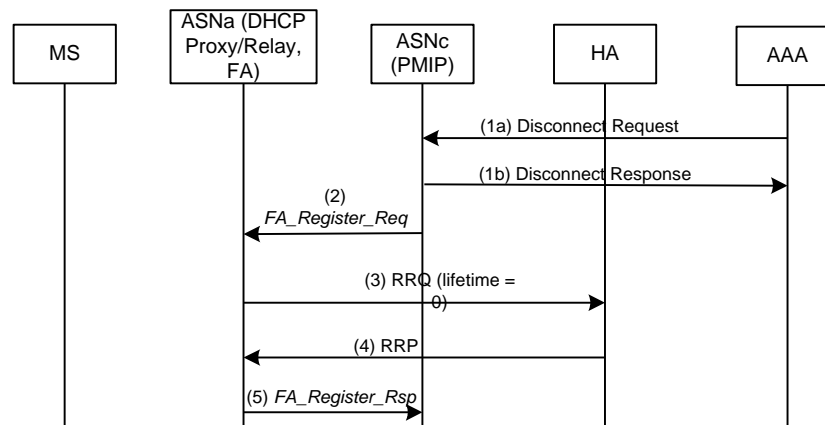


Figure 4-133 – PMIP4 Session Release triggered by Authenticator or AAA

##### STEP 1

The trigger can be Authenticator timeout on re-authentication or AAA initiated Disconnect. In the case of RADIUS, a RADIUS Disconnect Message is sent to the ASNc, which replies with A Disconnect ACK or NAK message. In the case of Diameter, a WiMAX-Abort-Session-Request command is sent to the ASNc to which the ASNc responds with a WiMAX-Abort-Session-Answer command indicating acceptance or rejection.

##### STEP 2

The ASNc where the PMIP4 client resides, sends a *FA\_Register\_Req* with the encapsulated RRQ of lifetime=0 to the ASNa where the FA resides, and a timer  $T_{FA\_Register\_Req}$  is started at this point by PMIP4 client to monitor *FA\_Register\_Rsp* message.

##### STEP 3

FA sends the RRQ with lifetime=0 to the HA.

##### STEP 4

The HA removes the binding and replies with RRP.

##### STEP 5

ASNa sends a *FA\_Register\_Rsp* with the encapsulated RRP to the PMIP4 client, and PMIP4 client stops  $T_{FA\_Register\_Request}$  once it gets *FA\_Register\_Rsp*.

#### 4.8.2.4.7.1.4.1 Authenticator or AAA Initiated PMIP4 Session Release Timer and Timing Consideration

This section identifies the timer used in the Authenticator or AAA Initiated PMIP4 Session Release procedure.

- $T_{FA\_Reg\_Req}$ : this timer is defined in section 4.8.2.3.7.1.1.

#### 4.8.2.4.7.1.4.2 Authenticator or AAA Initiated PMIP4 Session Release Error Conditions

This section describes error conditions associated with the Authenticator or AAA Initiated PMIP4 Session Release procedure.

#### 4.8.2.4.7.1.4.2.1 Timer Expiry

Table 4-132 shows details on 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 4-132.

**Table 4-132 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T <sub>FA_Register_Req</sub>	PMIP4 client	Behaves as if PMIP4 session has been released.

### 4.8.2.5 Proxy MIP4 R3 Mobility Management for MIP-based Ethernet Services

This section describes procedures between ASN and CSN for setting up the R3 connectivity for Ethernet services based on PMIP4 protocol. The overview and the message flows are provided in the stage 2 specification, while this section focuses on specifying the exact requirements on involved network entities.

The main difference between the PMIP4 based R3 establishment for Ethernet services and PMIP4 based R3 establishment for IP services is that in case of Ethernet services the R3 connection setup does not include the allocation and assignment of the IP address to the MS and hence the DHCP Proxy/relay/server entities are not involved in connection establishment. The mobility binding in case of Ethernet services contains the MS MAC address instead of the home IP address. The HA and the FA intercept the Ethernet frames destined for the registered MAC address and tunnel them over the MIP tunnel between the FA and the HA.

#### 4.8.2.5.1 Connection Setup Phase for MIP-based Ethernet Services

During the initial network entry, PMIP4 Client, Authenticator and FA are all collocated in the same network node.

The node requirements to support the R3 connection setup and management for Ethernet services are described as follows.

##### 4.8.2.5.1.1 Authenticator Requirements

Upon receiving the final RADIUS Access-Accept packet or Diameter WDEA command indicating EAP success, and if the MS is authorized for MIP-based Ethernet services, after the ETH ISF setup the authenticator SHALL trigger the collocated PMIP4 client.

##### 4.8.2.5.1.2 PMIP4 Client Requirements

Upon receiving an internal trigger from a collocated authenticator, the PMIP4 Client SHALL proceed with the Mobile IPv4 registration process on behalf of the authenticated MS. The Registration Request message SHALL be formatted and processed as described in section 4.8.2.1.3 with additional considerations as described here.

The PMIP4 client SHALL support the Proxy Mobile IPv4 Device ID Extension as defined in draft-leung-mip4-proxy-mode-08 [92] and SHALL include the Proxy Mobile IPv4 Device ID Extension in the Registration Request message. The PMIP4 client SHALL set the ID-Type in the Proxy Mobile IPv4 Device ID option to 1 and the Identifier field to the value of the MS MAC address.

The PMIP4 client SHALL support the GRE Key extension as defined in draft-yegani-gre-key-extension-03 [91]. When the PMIP4 client is triggered by the authenticator, it allocates a unique GRE key for the MS and saves it as part of the MS context. When the PMIP4 client sends the Registration Request message to the HA, it SHALL request the GRE encapsulation and SHALL include the GRE Key extension in the message and set it to the allocated GRE key for this MS.

During network access authentication, there may be two HA addresses downloaded to the Authenticator, as well as two MN-HA keys for PMIP4. The PMIP4 Client SHALL use a local policy to determine which HA to send the Registration Request message, and the corresponding MN-HA key to use.

1 The Registration Request message is protected with the MN-HA AE as described in section 4.8.2.1.3.

2 Upon receiving a MIP4 Registration Reply message from the Home Agent, the PMIP4 Client SHALL validate the  
3 message as described in section 4.8.2.1.3. If the message validation fails, the PMIP4 Client SHALL notify the  
4 collocated authenticator that the MIP4 authentication failed.

5 The PMIP4 client SHALL verify that the Registration Response indicating successful registration contains the GRE  
6 key extension. The PMIP4 client SHALL save the GRE key received from the HA as part of the MS context. If the  
7 Registration Response does not contain the GRE Key extension, the PMIP4 client SHALL inform the collocated  
8 authenticator that the R3 establishment failed.

9 The PMIP4 client SHALL verify that the Registration Response indicating successful registration contains the Proxy  
10 Mobile IPv4 Device ID Extension. The ID-Type in the Proxy Mobile IPv4 Device ID option MUST be set to 1 and  
11 the Identifier field MUST be set to the value of the MS MAC address that was included in the Registration Request  
12 message.

13 Upon receiving the Registration Response message with the Proxy Mobile IPv4 Device ID Extension included, the  
14 PMIP4 client SHALL ignore the Home address filed in the Registration Response message.

15 If the Proxy Mobile IPv4 Device ID extension is not included in the Registration Reply message, the PMIP4 client  
16 SHALL assume that the HA does not provide support for Ethernet services as described here and SHALL inform the  
17 authenticator that the R3 connection establishment was not successful. If the reply code in the Registration Reply  
18 message indicated successful registration, but the Proxy Mobile IPv4 Device ID extension was absent from the  
19 Registration Reply message, the PMIP4 client SHALL initiate the MIP4 de-registration as described in section  
20 4.8.2.4.7.1.2.

#### 21 **4.8.2.5.1.3 FA Requirements**

22 The FA SHALL operate as defined in section 4.8.2.1.3, with additional considerations as described in this section.

23 The FA SHALL support GRE encapsulation between the FA and the HA and it SHALL support the GRE key  
24 extension as defined in draft-yegani-gre-key-extension-03.

25 When encapsulating the user plane traffic, the FA SHALL use the GRE key from the MS context to fill in the value  
26 of the GRE Key in the uplink packet.

27 When receiving the downlink traffic from the HA, the FA SHALL use the GRE key from the downlink packet to  
28 locate the MS to which this packet SHALL be delivered.

#### 29 **4.8.2.5.1.4 HA Requirements**

30 The HA SHALL operate as described in section 4.8.2.1.3 and in this section.

31 The HA SHALL support GRE encapsulation between the FA and the HA and it SHALL support the GRE key  
32 extension as defined in draft-yegani-gre-key-extension-03.

33 The HA validates the Registration Request message and the MN-HA AE as described in section 4.8.2.1.3.

34 When the HA receives a Registration Request message containing the Proxy Mobile IPv4 Device ID Extension, the  
35 HA SHALL verify that the ID-Type in the Proxy Mobile IPv4 Device ID option is set to 1. It then extracts the MS  
36 MAC address from the identifier field of the Proxy Mobile IPv4 Device ID Extension and saves it as part of the MS  
37 context.

38 When the HA receives the Registration Request message with the GRE Key extension and if the message also  
39 contains the Proxy Mobile IPv4 Device ID Extension, the HA SHALL save the received GRE key as part of the MS  
40 context. The HA SHALL use the received GRE key for encapsulating the downlink traffic tunneled to the FA.

41 If the HA receives a Registration Request message where the Proxy Mobile IPv4 Device ID extension is included  
42 but the requested encapsulation method is not GRE or the GRE key extension is missing, the HA SHALL reject  
43 such Registration Request.

1 If the Registration Request message contains the Proxy Mobile IPv4 Device ID Extension the HA SHALL disregard  
2 the Home address filed in the Registration Request message and SHALL set the Home address filed in the  
3 Registration Response message to the ALL-ZERO-ONE-ADDR.

4 The HA protects the Registration Response message with the MN-HA AE as described in section 4.8.2.1.3.

5 When sending the Registration Response message, the HA SHALL include the Proxy Mobile IPv4 Device ID  
6 Extension and the GRE Key extension. The Proxy Mobile IPv4 Device ID Extension SHALL be set to the same  
7 value as in the corresponding Registration Request message. The HA SHALL generate the GRE key used to mark  
8 the uplink traffic and save it as part of the MS context. The HA SHALL set the GRE Key extension in the  
9 Registration Response message to the value of this GRE key.

#### 10 **4.8.2.5.1.5 AAA Server Requirements**

11 The AAA server requirements and the interface between the HA and the AAA server are as described in the section  
12 4.8.2.1.3. of the baseline specification.

#### 13 **4.8.2.5.2 Session Renewal for Ethernet Services**

14 Session renewal for Ethernet service is as described in the Figure 4-126 in section 4.8.2.2 of the baseline stage 3  
15 specification.

#### 16 **4.8.2.5.2.1 FA Requirements**

17 If the Proxy Mobile IPv4 Device ID Extension and the GRE Key extension were included in the initial Registration  
18 Request message that created the mobility binding, then the FA SHALL include the Proxy Mobile IPv4 Device ID  
19 Extension and the GRE Key extension in every subsequent Registration Request message.

20 When extending the mobility binding, the FA SHALL include the same values for the MAC address and the GRE  
21 key in the Registration Request message that were used during the initial registration. The Home address field in the  
22 Registration Request is set to the same value as in the initial Registration Request message.

23 The rest of the FA requirements are the same as in the section 4.8.3.1.2 of this document.

#### 24 **4.8.2.5.2.2 HA Requirements**

25 If the HA included the Proxy Mobile IPv4 Device ID Extension and the GRE Key extension in the initial  
26 Registration Response message when the mobility binding was created, then the HA SHALL include the Proxy  
27 Mobile IPv4 Device ID Extension and the GRE Key extension in every subsequent Registration Response message.

28 The Home address field in the Registration Response is set to the same value as in the initial Registration Response  
29 message.

30 The rest of the HA requirements are the same as in the section 4.8.3.1.3 of this document.

#### 31 **4.8.2.5.3 CSN-anchored Mobility Management Handover for MIP-based Ethernet Services**

32 The procedures for CSN-anchored mobility management are as described in the section 4.8.2.3.7 of the stage 3  
33 baseline document and as amended here.

34 The serving ASN SHALL include the Uplink R3 GRE key and Downlink R3 GRE key as part of the MIP4 Info  
35 provided to the Target ASN during the CSN-anchored handover.

36 The target ASN SHALL save the Uplink R3 GRE key and Downlink R3 GRE key as part of the MS context.

37 When the target ASN receives the Uplink R3 GRE key and Downlink R3 GRE keys during the MS handover, the  
38 target ASN SHALL use the GRE encapsulation on the R3 interface towards the HA.

39 When encapsulating the uplink traffic, the target ASN SHALL use the Uplink R3 GRE key to fill in the Key field in  
40 the GRE header.

41 When receiving the packet from the HA, the target ASN SHALL match the Downlink R3 GRE Key from the MS  
42 context with the GRE key from the packet header to determine the MS to which the packet SHALL be delivered.



#### 4.8.2.5.4 Session Termination for Ethernet Services

When the Ethernet session is terminated the R3 connection between the FA and the HA must be removed. Session removal handling in case of Ethernet services is the same as the session removal for IP services and is described in the baseline stage 3 specification, sections 4.8.2.4.7.1.2 (ASN Initiated PMIP4 Session Release), 4.8.2.4.7.1.3 (HA Initiated PMIP4 Session Release) and 4.8.2.4.7.1.4 (R3 Session Release – Initiated by Authenticator or AAA).

When sending a message to remove the R3 connection related to Ethernet services, the PMIP4 client and the HA SHALL include the Proxy Mobile IPv4 Device ID Extension in the message. The PMIP4 client and HA SHALL handle the Home address field as described in section 4.8.3.1 of this specification.

When the Registration Revocation message is sent for the session related to Ethernet services, it SHALL contain the Proxy Mobile IPv4 Device ID Extension carrying the MAC address of the MS. Likewise, the Registration Revocation Acknowledgment message SHALL contain the Proxy Mobile IPv4 Device ID Extension identifying the MS whose session is revoked.

#### 4.8.2.5.5 Data plane handling

The PMIP4 client indicates that the MIP4 session is related to the Ethernet services by including the Proxy Mobile IPv4 Device ID Extension into the Registration Request message. When the HA accepts such a Registration Request, it SHALL process the data plane as described in this section.

The R3 data plane delivery mechanism between the FA and the HA is based on GRE over IP and the GRE encapsulation SHALL be negotiated during the MIP registration. The data plane SHALL be encapsulated in a GRE header and the GRE payload is the Ethernet frame.

The encapsulating entity SHALL set the GRE key field in the GRE header to the GRE key value received from the peer entity during the Mobile IPv4 registration process.

The HA SHALL intercept any Ethernet frame coming out of the CSN bridge port, which is registered by the mobility binding to the MAC address of the associated MS, and SHALL tunnel it to the current FA of the MS using GRE encapsulation.

The mobility binding of the MS is identified by the GRE key contained in the transferred packet. When receiving the downlink packet, the FA SHALL use the GRE key from the GRE header of the received packet to identify the MS to which the packet has to be delivered.

In the uplink, the FA SHALL use the GRE key identifying the mobility binding of the originating MS of the Ethernet frame for sending the Ethernet frame upstream. The HA SHALL forward the Ethernet frame received from the FA to the CSN bridge port, which is registered by the mobility binding to the MS-ID identified by the GRE key contained in the packet.

### 4.8.3 Client MIP4 R3 Mobility Management

The basic client MIP4 operation SHALL be as per Mobile IP standard RFC 3344 and RFC 3024. All traffic from MIP4 client with Home Address as source address and destined to an address other than the Foreign Agent, will be reverse tunneled back to Home Agent. For sending multicast and broadcast packets between home network and the MIP4 client, the MIP4 client SHALL follow RFC 3024. In order to send multicast and broadcast packets to the home network from the client node, encapsulating delivery method SHALL be negotiated. If encapsulating delivery mode is negotiated between the FA and the MIP4 client, then all traffic including unicast packets will be tunneled to the FA. If the encapsulating delivery negotiation fails for some reason, the foreign agent will assume the direct delivery method (no encapsulation from MN to FA). In such case, multicast/broadcast packets with home-address as source address will be dropped by the foreign agent. This specification assumes that the Home agent is situated at the home network (HCSN or VCSN) which is topologically separate from the foreign network and the home agent must act as a multicast router (RFC3024).

The following sections describe the detailed stage-3 node requirements for each phase of the user's session via CMIP4.

The CMIP4 behavior for interworking with 3GPP2 is described in the Stage 3 Annex, WiMAX – 3GPP2 Interworking.

#### 4.8.3.1 Client MIP4 Connection Setup Procedure

The basic connection setup procedure using CMIP4 is shown in stage-2, section 7.8.1.9.1. The node requirements to support the connection setup are described as follows.

##### 4.8.3.1.1 MS Requirements

The Mobile IPv4 Client behavior assumes that the Mobility Stack in the MS conform to IETF standards such as [48].

Due to the EAP based method of bootstrapping Mobility Keys, after successful Device/User Network Access 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-Identity 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 Identity@realm that was used as the Outer-Identity 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. Additionally, if MN-FA AE is used, the Mobile IPv4 Client SHALL use the same value of SPI-CMIP4 for MN-FA SPI. This is in accordance with the same behavior specified on the FA side in section 4.3.1.2. During the initial MIP registration, the MS may use dynamic HA assignment and/or dynamic HoA address assignment. If the MS desires a dynamic home address assignment by the home agent, it SHALL include 0.0.0.0 in the HoA field of the RRQ. 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). 255.255.255.255 in the HA field means the MS prefers an HA assignment in the home domain, while 0.0.0.0 means the MS has no preference for home vs. visited domain assignment.

The MS may also use a combination of dynamic HoA address assignment and dynamic HA assignment to cover different scenarios such as:

- Dynamic HoA, dynamic HA;
- Static HoA, dynamic HA;
- Dynamic HoA, static HA;
- Static HoA, static HA.

In the last two cases with static HA, the RRQ is likely to be rejected by the network and the MS may have to re-register using the first two cases with dynamic HA. In the case of static HoA with dynamic HA, the static HoA can only be provided as a hint by the MS. The HoA MUST be updated with the assigned value once the RRP with success code is received.

MS requesting dynamic home agent assignment SHALL use the MN-HA key that is derived based on ALL-ZERO-ONE-ADDR 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.

If the Mobile IP Client has access to the address of the Home Agent, i.e., the static HA case, 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).

- 1 The MN-FA Challenge Extension as specified in [42] is not supported.
- 2 The error handling and retransmission behavior of the MS SHALL be governed by the Mobile IPv4 standard [48].
- 3 When connected to a WiMAX network, if the MS wants to use CMIP4 it SHALL NOT invoke DHCP for IPv4  
4 address acquisition before and after starting the Mobile IP procedures.
- 5 The scenario when the MS performs CMIP4 registration after the network performs PMIP4 procedures is not in the  
6 scope of this Release. In other words, in this Release once the MS sends DHCPREQUEST, it is not expected to  
7 follow it later on with MIP RRQ messages.

#### 8 **4.8.3.1.2 FA Requirements**

9 FA and anchor DPF are always collocated. As soon as the FA (collocated with the DPF) determines that the data  
10 path (i.e., R6) is connected for a new MS for which no mobile IPv4 session exists, the FA SHALL send a series of  
11 Agent Advertisement over that data path (i.e., R6) to the MS after a configurable time period (to allow the MS to  
12 initiate either Simple IPv4 or CMIP4). The Agent Advertisement SHALL contain the FA-CoA and the supported  
13 lifetime. The FA SHALL set the MIP lifetime < AAA session time attribute value that the FA is configured to  
14 support. The Agent Advertisement SHALL be formatted as per [48] The FA SHALL support MIP4 registration  
15 revocation as per [50] and the FA SHALL set the appropriate fields in the Agent Advertisement message.

16 The FA SHALL send Agent Advertisement under the following conditions:

- 17 a. The DPF notifies the FA that the data path (i.e., R6) is up and the FA determines that the MS is authorized for  
18 only CMIP4 from the subscriber profile which may be cached in the NAS (received during user/device  
19 authentication from the HAAA).
- 20 b. The DPF in the target ASN forwards the Anchor DPF *HO\_Req* received over R4 to the target FA. Note that  
21 the currently serving ASN is responsible for ensuring that the MS is a CMIP4 authorized MS and the MS  
22 has an active CMIP4 session. The target FA does not perform additional MS capability checks before  
23 sending Agent Advertisement.
- 24 c. When solicited by the MS unless the MS has an existing IPv4 session.

25 Upon receiving the RRQ message from the MS, with a static HA field, the FA SHALL relay the RRQ to the  
26 requested HA. If the HA field in the RRQ doesn't match the visited HA or the home HA address downloaded during  
27 access authentication, the FA SHALL reject the RRQ with an error code 136 (unknown home agent address). The  
28 MS may then retry using dynamic HA assignment.

29 If the MS has requested dynamic HA assignment by specifying the HA field as ALL-ZERO-ONE-ADDR, the FA  
30 SHALL relay the RRQ to the visited HA if there is visited HA address downloaded during access authentication  
31 AND if the HA field in the RRQ is all '0'. Otherwise, the FA relays the RRQ to the home HA address downloaded  
32 during access authentication.

33 To identify the radio access technology (RAT) used in the ASN, the FA SHOULD append to the RRQ the PMIP  
34 Access Technology Type Extension defined in PMIP4 (draft-leung-mip4-proxy-mode-05.txt) to indicate which  
35 access type is being used, before relaying the RRQ to the HA.

36 If GRE tunneling is used between the FA and the HA, the FA MAY include the GRE key extension CVSE carrying  
37 its GRE-key as defined in draft-yegani-gre-key-extension-03.txt.

38 Upon receiving the RRP back from the HA, the FA SHALL forward the RRP to the MS if FA-HA AE validation is  
39 successful (if FA-HA AE is used). If FA-HA AE is not used, the FA SHALL forward the RRP back to the MS.

40 The Registration Revocation message SHALL be either protected using an FA-HA Authentication Extension as per  
41 [50] or by using another security mechanism at least as secure, and agreed upon by the home and visited domains,  
42 e.g., IPsec. If an FA-HA security association is not available, or in the absence of another appropriate security  
43 mechanism, the FA and HA SHALL silently discard any Registration Revocation messages received.

44 If there is no alternative way to secure FA-HA communication other than FA-HA AE, the FA SHALL extract the  
45 FA-HA key from the security context and append the FA-HA AE in the relayed RRQ.

#### 4.8.3.1.3 HA Requirements

The HA SHALL process Mobile IPv4 message as per [48]. Upon receiving an RRQ if the HA does not have a security association for the MN, the HA SHALL issue a RADIUS Access-Request or Diameter WHA4R command with User-Name attribute set to the contents of the NAI extension received in the RRQ. The RADIUS Access-Request or Diameter WHA4R command is routed through VAAA if the HA is located in the visited network. After successful processing of the RADIUS Access-Request or Diameter WHA4R command, the HAAA responds back to the HA with the set of attributes including the mobility keys (MN-HA, HA-RK) and associated SPI values, so that the HA can validate the corresponding Authentication Extensions in the RRQ. The same SPI value and the MN-HA key are used for both verifying incoming RRQs and signing outgoing RRs by the HA.

If the Mobile requested Dynamic HA assignment by setting the HA-IP address in the RRQ to the ALL-ZERO-ONE-ADDR then the FA simply forwards the RRQ to the HA address that it received during Device/User Network Access Authentication and Authorization. In this case the HA receives the RRQ with the HA field set to ALL-ZERO-ONE-ADDR in the message body and the packet is destined to its IP address. The HA SHALL indicate this to the HAAA by including the RRQ-HA-IP attribute set to the Home Agent field of the RRQ in RADIUS Access-Request or Diameter WHA4R command. In response to RADIUS Access-Request or Diameter WHA4R command, HA will receive RADIUS Access-Accept or Diameter WHA4A command with RRQ-MN-HA-KEY from the HAAA that is calculated based on RRQ-HA-IP address as well as MN-HA-CMIP4 key that is calculated based on HA-IP-MIP4 address. The HA SHALL use the RRQ-MN-HA-KEY for validation of MN-HA authentication extension in the received RRQ and the MN-HA-CMIP4 key for deriving MN-HA authentication extension in the RRP it sends to the MS. For MIP re-registration, the HA SHALL use only MN-HA-CMIP4 key for validation of RRQ and deriving MN-HA authentication extension in RRP.

If the FA-HA AE (if required) and MN-HA AE (required) validations are successful, the HA SHALL assign an HoA to the MS if dynamic HoA assignment is requested (i.e., RRQ contains the HoA=0.0.0.0) and respond back to the MS with a RRP indicating success. If the RRQ contains a non-zero HoA, then the HA SHALL authenticate the MIP Registration Request and upon success the HA SHALL register the mobility binding with that HoA. If the RRQ contains the GRE key extension CVSE the HA SHALL respond back to the FA with GRE key extension CVSE carrying its GRE-key in the RRP.

The HA SHALL exchange the revocation support extension with the FA as defined in [50]. The generic error handling requirements for the HA are as per [48].

#### 4.8.3.1.4 AAA Server Requirements

In addition to the requirements listed in section 4.8.2.1.6, if the RADIUS Access-Request Diameter WHA4R command from HA contains a RRQ-HA-IP field, the HAAA SHALL derive an additional key RRQ-MN-HA-KEY using the key derivation formula for MN-HA-CMIP4 in section 4.3.5.1 but with RRQ-HA-IP as the HA-IPv4 address. The HAAA SHALL send back both RRQ-MN-HA-KEY and MN-HA-CMIP4 key to the HA in the RADIUS Access-Accept or Diameter WHA4A command.

#### 4.8.3.2 Client MIP4 Session Renewal

The Mobile IPv4 session SHALL be renewed by the MS based on the registration lifetime value in the RRP. The processing requirements for the resulting RRQ and RRP are the same as defined in section 4.8.2.1.3.

##### 4.8.3.2.1 CMIP4 Session Renewal Procedure

Same as the CMIP4 session establishment procedure described in section 4.8.3.1.

#### 4.8.3.3 Client MIP4 CSN Anchored Mobility Handover

The CSN anchored mobility event MAY be triggered by two different events:

- The MS incurring a handover to a target BS which requires a relocation of the FA function (CoA) due to network boundary crossing or network configuration;
- Due to resource management decision in the ASN-GW the ASN-GW MAY force a relocation of the MIP4 service to a different FA.

#### 4.8.3.3.1 MS Requirements

A CMIP4 capable MS SHALL send a Mobile IPv4 RRQ to the FA after it receives an Agent Advertisement from the FA containing a new FA-CoA after incurring inter BS handover. The mobile IPv4 registration requirements are as per section 4.8.2.1.3.

#### 4.8.3.3.2 FA Requirements

If the target ASN initiates the FA relocation negotiation (Pull Mode), it sends an Anchor\_DPF\_HO\_Trigger message to the Anchor ASN. If Anchor ASN agrees with the FA relocation, it sends an Anchor DPF\_HO\_Req message to the Target ASN. If Anchor ASN initiates FA relocation negotiation (Push Mode), it sends an Anchor DPF\_HO\_Req message to Target ASN, the Target FA SHALL send an Agent Advertisement to the MS as soon as the data path to the MS is established.

**Table 4-133 – Anchor\_DPF\_HO\_Req Message**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>Authenticator ID	5.3.2.19	O	
>Anchor MM Context	5.3.2.11	M	MIP4 Info, etc.
>>MS Mobility Mode	5.3.2.104	M	This TLV SHALL be set to indicate CMIP4.
>>MIP4 Info	5.3.2.96	O	
>>>HA IP Address	5.3.2.75	O	
>>>Care-of Address (CoA)	5.3.2.28	O	
>PPAQ	5.3.2.131	O	Used during PPA Relocation. This TLV (both expended and the original Quota) SHALL be included if online accounting is activated in the Serving ASN.
>>Quota Identifier	5.3.2.148	CM	This TLV SHALL be included if PPAQ is included in the transmitted message.
>>Volume Quota	5.3.2.167	O	
>>Volume Threshold	5.3.2.168	O	
>>Volume Used	5.3.2.357	O	
>>Duration Quota	5.3.2.275	O	
>>Duration Threshold	5.3.2.276	O	
>>Resource Quota	5.3.2.277	O	
>>Resource Threshold	5.3.2.278	O	
>>Update Reason	5.3.2.279	O	
>>Service-ID	5.3.2.280	O	
>>Rating-Group-ID	5.3.2.281	O	
>>Termination Action	5.3.2.282	O	
>>Pool-ID	5.3.2.283	O	
>>Pool-Multiplier	5.3.2.284	O	

IE	Reference	M/O	Notes
>>Prepaid Server	5.3.2.285	O	This TLV SHOULD be included if available (provided by HAAA).
>>SFID (one or more)	5.3.2.184	O	SF ID(s) SHALL be included in flow based prepaid accounting scenario.
PPAC	5.3.2.65	O	Describes the Prepaid Capabilities of the ASN. This TLV SHALL be included if online accounting is activated in the Serving ASN for the particular MS session. If Target ASN does not support any of the required online accounting capabilities, it SHOULD reject Anchor DPF relocation procedure.
>AvailableInClient	5.3.2.89	CM	This TLV SHALL be included if PPAC is included in the transmitted message.

In response to the Anchor DPF *HO\_Req* message the target FA SHALL respond to the ASN functional entity with an Anchor DPF *HO\_Rsp* message described in Table 4-93. The further processing of the resulting RRQ and RRP at the target FA for the MS is as per section 4.8.2.1.4.

After the CSN anchored handover is successfully completed the target FA function SHALL send the Context\_Rpt message to the anchor authenticator function. The Context\_Rpt message must contain the address of the new anchor DPF function. Upon receipt of the Context\_Rpt message containing the address of the new anchor DPF the anchor authenticator must update its notion of the location of the anchor DPF function for this MS. The anchor authenticator SHALL confirm the receipt of the Context\_Rpt message by sending the Context\_Ack message.

After the CSN anchored handover is successfully completed, the target FA SHALL send the Context\_Rpt message to the serving BS. The Context\_Rpt message must contain the address of the new anchor DPF function. Upon receipt of the Context\_Rpt message containing the address of the new anchor DPF, the serving BS must update its notion of the location of the anchor DPF function for this MS. The serving BS 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 MIP4 session setup, the HA SHALL remove the binding with CoA of the Anchor FA when it receives a registration revocation message ([50]) 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 [50].

#### 4.8.3.3.7 CMIP4 Mobility Procedure

##### 4.8.3.3.7.1 CMIP4 CSN MM Handover

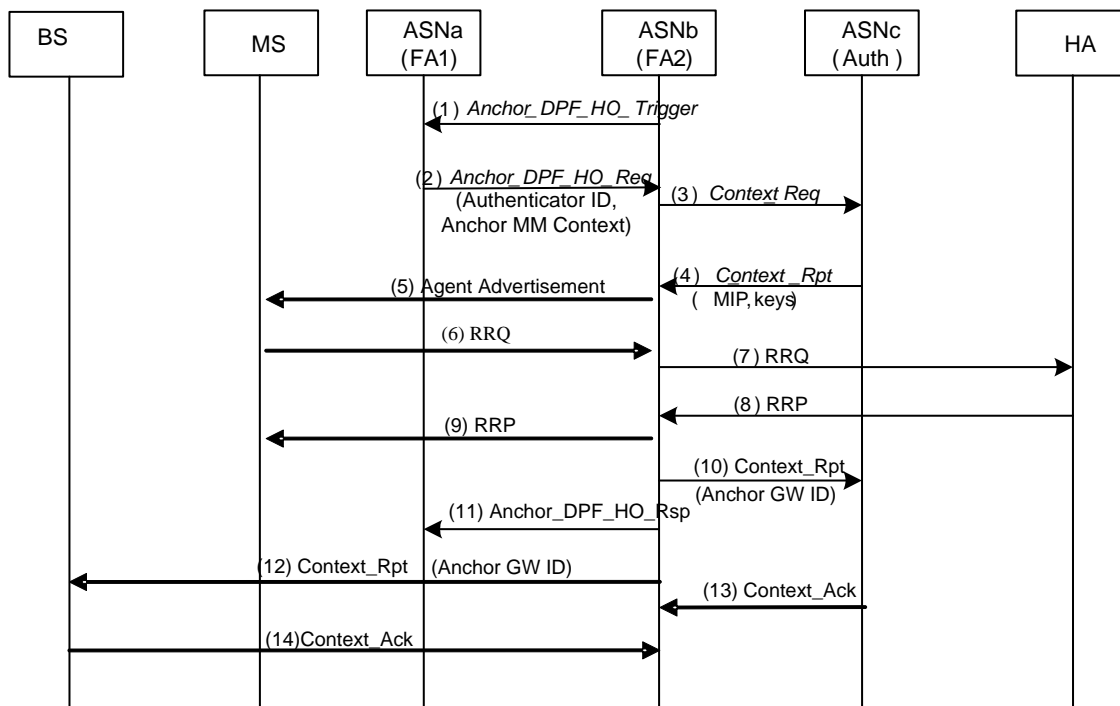


Figure 4-134 – CSN-Anchored Mobility (CMIP)

#### STEP 1

If the target ASNb initiates the FA relocation negotiation (Pull Mode), it sends an *Anchor\_DPF\_HO\_Trigger* message to the anchor DPF in ASNa. The details of the *Anchor\_DPF\_HO\_Trigger* are provided in Table 4-92. If ASNa agrees with the FA relocation, it proceeds to Step 2. After sending *Anchor\_DPF\_HO\_Trigger*, ASNb starts a timer  $T_{Anchor\_DPF\_HO\_Trigger}$  for *Anchor\_DPF\_HO\_Req*. Once *Anchor\_DPF\_HO\_Req*, indicating the FA relocation decision of ASNa, is received by ASNb,  $T_{Anchor\_DPF\_HO\_Trigger}$  is stopped.

If the source ASNa initiates the FA relocation procedure (Push Mode), the call flow starts from Step 2.

#### STEP 2

ASNa sends an *Anchor\_DPF\_HO\_Req* message to the DPF in ASNb. The message contains the current Anchor MM context information for the MS and the Authenticator Id and ASNa will start a timer  $T_{Anchor\_DPF\_HO\_Req}$ <sup>20</sup> for *Anchor\_DPF\_HO\_Rsp* from ASNb.

If *Anchor\_DPF\_HO\_Trigger*(ASNb) and *Anchor\_DPF\_HO\_Req*(ASNa) are triggered independently and ASNa sees *Anchor\_DPF\_HO\_Trigger* arriving after sending of the *Anchor\_DPF\_HO\_Req* between steps 2 and 11 ASNa just ignores this message. ASNb will see and process *Anchor\_DPF\_HO\_Req* arriving after the sending of *Anchor\_DPF\_HO\_Trigger*. (normal situation).

#### STEP 3

If the Target ASN does not accept FA relocation it proceeds directly to Step 11.

<sup>20</sup>  $T_{Anchor\_DPF\_HO\_Req}$  value should be larger than the sum of  $T_{R4\_Cntxt\_Req}$  including retransmissions and time taken to register with HA.

Target ASN for obtaining MIP keys sends a *Context\_Req* message to the Authenticator GW, and starts a timer  $T_{R4\_Cntxt\_Req}$  for *Context\_Rpt*. This message relays some information about target ASN that is necessary in order to construct MIP Keys.

#### STEP 4

Authenticator GW sends *Context\_Rpt* that contains the FA-HA and MN-FA MIP keys if these key are used. This message is sent to the Target ASN, whose address was identified as the source address of the *Context\_Req* message in step 3.

#### STEP 5

After receiving *Context\_Rpt*, ASNb stops  $T_{Cntxt\_Req}$ . ASNb sends Agent Advertisement to MS.

#### STEP 6-9

The MS responds with RRQ. ASNb relays RRQ to HA after validating MN-FA authentication extension (if required) and appending FA-HA authentication extension. HA responds with RRP. ASNb relays RRP to MS. At this point, ASNb gets registered with HA.

#### STEP 6

ASNb sends Context Report to the Authenticator GW. The *Context\_Rpt* message contains the address of the new anchor DPF function.

#### STEP 7

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.

If the Target ASN does not accept FA relocation it responds with an *Anchor\_DPF\_HO\_Rsp* message with *Accept/Reject Indicator* indicating Reject. ASNa also stops  $T_{Anchor\_DPF\_HO\_Req}$  started in step 2.

#### STEP 8

ASNb sends Context Report to the BS. The *Context\_Rpt* message contained the address of the new anchor DPF function.

#### STEP 9

Upon receipt of the *Context\_Rpt* message containing the address of the new anchor DPF the anchor authenticator updates its notion of the location of the anchor DPF function for this MS. The anchor authenticator confirms the receipt of the *Context\_Rpt* message by sending the *Context\_Ack* message.

#### STEP 10

BS also updates location of the anchor DPF function for this MS upon receipt of the *Context\_Rpt* message. The BS confirms the receipt of the *Context\_Rpt* message by sending the *Context\_Ack* message.

#### 4.8.3.3.7.1.1 CMIP4 CSNMM Handover Timers and Timer Considerations

This section provides the description of the timer used during CMIP4 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*.
- $T_{R4\_Cntxt\_Req}$ : is started by the target ASNb when the *Context\_Req* is sent on R4. It is stopped upon receiving a corresponding *Context\_Rpt*.



Table 4-134 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-134 – Timer Values for CMIP4 CSN MM Handover Messages over R4/R3**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
T <sub>Anchor_DPF_HO_Trigger</sub>	TBD		TBD
T <sub>Anchor_DPF_HO_Req</sub>	TBD		TBD
T <sub>R4_Cntxt_Req</sub>	TBD		TBD

#### 4.8.3.3.7.1.2 CMIP4 CSN MM Handover Error Conditions

This section describes error conditions associated with the CMIP4 CSN MM Handover procedure.

##### 4.8.3.3.7.1.2.1 Timer Expiry

Table 4-135 shows details on the corresponding actions associated with timer expiry. 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 4-111 Timer Expiry Conditions.

**Table 4-135 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T <sub>Anchor_DPF_HO_Trigger</sub>	Target FA	CMIP4 CSN MM handover is aborted and further action of Serving/Target FA is implementation Specific.
T <sub>Anchor_DPF_HO_Req</sub>	Serving FA	CMIP4 CSN MM handover is aborted and further action of Serving/Target FA is implementation Specific.
T <sub>R4_Cntxt_Req</sub>	Target FA	CMIP4 CSN MM handover is aborted and <i>Anchor_DPF_HO_Rsp</i> is sent to ASNa with Result Code set to Failure.

#### 4.8.3.4 Client MIP4 Session Termination

The ongoing MIP4 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 ([50]).

Based on what the I-bit setting in the Revocation Support Extension (sec 3.2, [50]) 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 [48].

The HA implementations compliant to this document SHALL support and use Mobile IPv4 Registration Revocation ([50]).

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 (optionally) and the NAS. In this case the Accounting Stop message SHALL contain the Terminate-Cause attribute set to User Request indicating that the session has been terminated and the MS left the network. In the case of Diameter, the accounting message WACR do not signal the termination of the session but instead, the HA signals the termination of the session by sending a WASR command to the AAA. Upon receiving RADIUS Accounting-Request Stop message, or Diameter WASR command, the HAAA SHALL signal the release of all state information and in particular the EAP server 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 [57]. As per [57] 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 [71].

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:

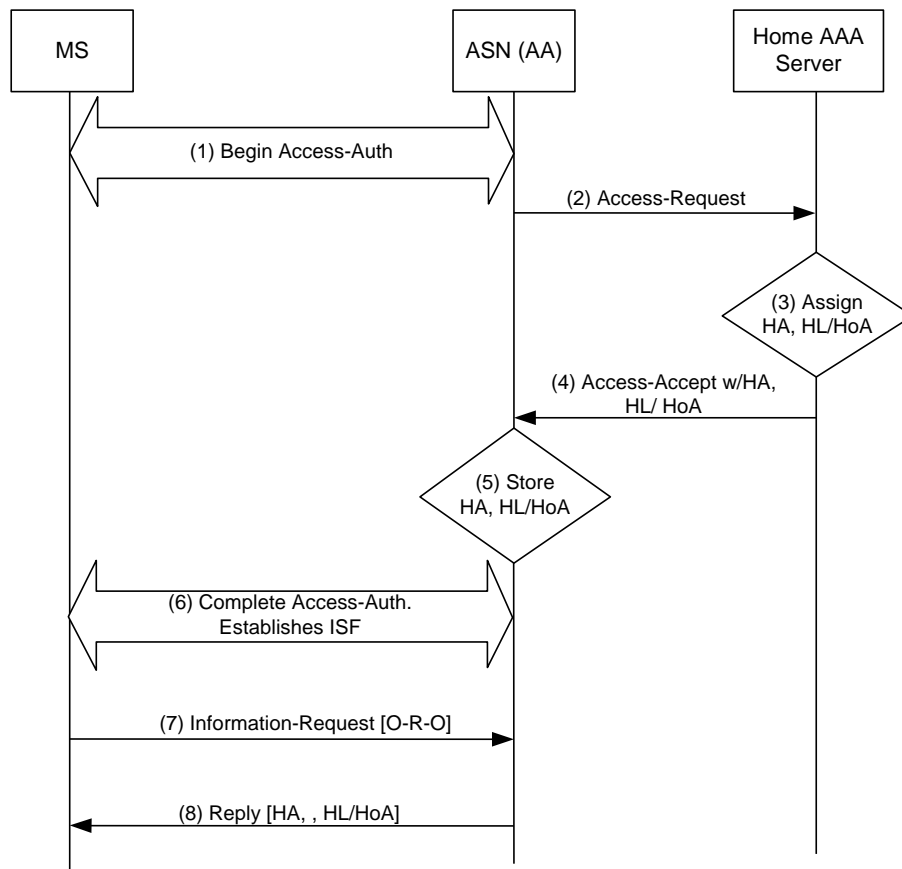
- [57]: Base MIP6 protocol
- [71]: Authentication Protocol for MIP6
- [69]: Identification Option for MIP6
- [69]: draft-ietf-mip6-hiopt-12.txt
- [84]: draft-ietf-dime-mip6-split-12.txt

#### 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 RADIUS Access-Accept packet or Diameter WDEA command 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 4-135:



**Figure 4-135 – Client MIP6 Connection Setup Procedure**

#### STEP 1

The MS performs Access Authentication procedure via EAP-PKMv2.

#### STEP 2

The NAS (which is the Anchor Authenticator (AA) in the ASN) sends an RADIUS Access-Request packet or Diameter WDER command to the Home AAA server.

#### STEP 3

While performing EAP authentication and authorization the Home AAA server notes that the user is authorized for MIP6 service by verifying the user's profile. The Home AAA server assigns an HA and either a HL prefix or a HoA to the MS.

**STEP 4**

The Home AAA server includes the following in a RADIUS Access-Accept or Diameter WDEA command: The Assigned Home Agent info in the MIP6-Home-Agent Address VSA/AVP, if HL prefix is assigned, HL prefix info in the MIP6-Home-Link Prefix VSA/AVP, if the HoA is assigned, HoA info in the MIP6-Home-Address VSA/AVP.

**STEP 5**

The Anchor Authenticator in the ASN receives these MIP6 bootstrap parameters via the related VSA/AVP s from the Home AAA server and stores them in the local DHCPv6 server.

**STEP 6**

The Access Authentication procedure completes successfully. The Initial Service Flow (ISF) gets established. The MS configures its IPv6 stack with a link local and global address as per the basic IPv6 connection setup procedure.

**STEP 7**

The MS requests the MIP6 bootstrap information using the DHCPv6 Information-request message [ 3736] sent to the ASN.

**STEP 8**

The ASN looks up the appropriate cached record based on the Path\_ID over which the DHCPv6 information request is received and replies back to the MS [RFC 3736] with the options that were requested and attaches the MIP6 bootstrap information options as per draft-ietf-mip6-hiopt-12.txt.

**4.8.4.1.1 MS/CMIP6 Client Operation**

MIP6 is an integral part of the IPv6 stack in the MS. The terms MS and CMIP6 Client are used interchangeably in this document. The CMIP6 Client SHALL initiate the Mobile IPv6 registration procedure as part of the connection setup as soon as the MS configures (either via DHCPv6 or via auto-configuration) a global scope IPv6 address when attached to the ASN. Local policy at the MS acts as the trigger for initiating the MIP6 binding update following the care-of-address configuration. The CMIP6 Client SHALL use the address obtained or auto-configured in the attached ASN as the Care-of Address (CoA) in the MIP6 Binding Update.

The MS discovers the address of the HA, its own HoA or HL prefix by including the option codes defined in [draft-jang-mip6-hiopt-02.txt] in the DHCP Information-Request message which is sent by the MS to the DHCPv6 proxy or relay in the ASN. In the DHCP Information Request, the MS may include the Home Network Identifier Option to identify the home network from which it wants to receive the bootstrap info. If used, the MS SHALL set the id-type to 1 in this option and include the @realm part of its NAI in the Home Network Identifier field.

After obtaining the HA address, via the DHCP response the CMIP6 Client SHALL send a BU (Binding Update) to the HA to register its binding with the CoA. The BU SHALL be protected by the Mobility Message Authentication Option as defined in [71]. The MS implementations conformant to this specification SHALL support MN-HA Mobility Message Authentication Option as the default mechanism. Use of other mechanisms to secure Mobile IPv6 signaling is not prohibited but outside the scope of this specification. An even-valued MN-HA SPI SHALL be used. The procedure to derive the MN-HA key to compute MN-HA Mobility Message Authentication Option is described in section 4.3.5.3. The MS SHALL include Mobile Node Identifier Option for Mobile IPv6 [69] in all BUs. The Mobile Node SHALL use the same pseudo Identity, i.e., pseudoIdentity@Realm that was used during Device/User Network Access Authentication and Authorization procedure at the ASN.

Note: Even-valued SPIs are also used for CMIP6. The reason for this is to avoid backwards-compatibility issues in future releases where, in addition to PMIP4, PMIP6 may be supported.

If the MS also received the HoA in the DHCP Reply message, the MS SHALL set the HoA field in the BU to the received HoA.

1 If the MS did not receive the HoA in the DHCP Reply message but it received the HL prefix info, the MS can  
2 perform stateless address auto-configuration of the HoA from the received HL prefix as per autoconfiguration  
3 process described in [78]. In this case, the MS SHALL set the HoA field in the BU to the auto-configured HoA.

4 If the MS did not receive the HoA and HL prefix in the DHCP Reply message, the MS SHALL either set the HoA  
5 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  
6 Interface ID (IID) in the HoA field. In the latter case, the MS is requesting the HA to assign a HoA using the IID  
7 supplied by the MS. The MS SHALL perform back processing as per [71]. The MIP6 Route optimization feature  
8 requires the existence of an IPsec SA between the MS and the HA. Since the Authentication protocol [71] is used for  
9 securing the registration messages, route optimization as described in [57] cannot be performed. Route optimization,  
10 in the scenario when the MS is using [71] for securing the CMIP6 registration messages, is for further study.

#### 11 **4.8.4.1.2 NAS and DHCPv6 Proxy Requirements**

12 The NAS in the ASN, is also the Anchor Authenticator and should cache the Mobile IPv6 bootstrap parameters that  
13 are received from the Home AAA server at the time of Device/User Network Access Authentication and  
14 Authorization procedure. Upon receiving DHCPv6 information request from the MS the DHCPv6 proxy SHALL  
15 reply to the MS with the Home Network Information option with the MIP6 bootstrap info that was received from the  
16 AAA server. To identify the set of information to convey to the MS, the DHCPv6 proxy SHALL use the R6  
17 Path\_ID to determine the set of cached parameters that is relevant to the MS. The DHCPv6 proxy may also receive  
18 the Home Network Identifier Option [88] in the DHCPv6 Information Request. However, the DHCPv6 proxy is not  
19 required to process this information. To convey the Home Agent address to the MS, the DHCPv6 proxy SHALL set  
20 the hainfo-type to 1 and the Home Network Information field to the Complete IPv6 address of the home agent in the  
21 Home Network Information Option. To indicate the received HL prefix, the DHCPv6 proxy SHALL set the hainfo-  
22 type to 0 and the Home Network Information field to Home subnet prefix in the Home Network Information Option.  
23 If both HA and HL prefix information need to be conveyed to the MS, the DHCPv6 proxy SHALL include two  
24 Home Network Information Options with fields set as described above.

#### 25 **4.8.4.1.3 HA Requirements**

26 The HA SHALL support Mobile IPv6 operation with Base Mobile IPv6 [57] and Authentication Protocol for Mobile  
27 IPv6 [71]. Upon receiving a BU from a MS, the HA SHALL perform validation of MN-HA Mobility Message  
28 Authentication Option based on the identification of the user from the NAI contained in the BU in the Mobile Node  
29 Identifier Option [69] and the corresponding MN-HA key. The HA acquires the MN-HA key from the AAA by  
30 sending a RADIUS Access-Request packet or Diameter WHA6R command as shown in Table 5-9/Table 5-34. The  
31 User-Name attribute value is obtained from the NAI contained in the BU in the Mobile Identifier Option [69]. This  
32 NAI SHALL be the same NAI used as the Outer-Identity during Device/User Network Access Authentication and  
33 Authorization procedures. The HA SHALL also include the following attributes/AVPs: the IPv6 address of the HA  
34 so that the HAAA can validate that the correct values have been used. The HA SHALL sign the RADIUS packet  
35 using Message-Authenticator as specified in [52].

36 If the HA requires the Chargeable User Identity (CUI) attribute, it SHALL include the CUI attribute/AVP set to  
37 NULL in the RADIUS Access-Request packet or Diameter WHA6R command.

38 The HA SHALL include the WiMAX-Capability attribute/AVP indicating its capabilities to the HAAA.

39 Upon successful processing by the HAAA, the HA receives a RADIUS Access-Accept packet as shown in Table 5-9  
40 or a Diameter WHA6A command as shown in Table 5-35. The HA SHALL validate the RADIUS Message-  
41 Authenticator as per the procedures defined in [52]. If the RADIUS packet does not contain the Message-  
42 Authenticator, the HA SHALL silently discard the packet. If the packet contains the Message Authenticator but the  
43 computed value does not match the Message Authenticator, then the HA SHALL silently discard the packet. If the  
44 HA discards the RADIUS Access-Accept packet it should also discard the BU message. If the RADIUS validation  
45 is successful, then the HA should decrypt the MN-HA attribute using the procedures defined in [39] section 3.5.

46 Once the MN-HA key is obtained, the HA can validate the MN-HA AE. If the MN-HA AE is verified successfully,  
47 the HA SHALL create a security association with the MN storing the MN-HA key locally. The HA SHALL use the  
48 MN-HA key to compute MN-HA AE for all subsequent messages. Once the MN-HA AE is validated the HA  
49 SHALL continue to process the BU as prescribed below:

- If the MN-HA AE fails authentication, the HA SHALL silently discard the BU.

- 1       • If the RADIUS Access-Accept packet or Diameter WHA6A command contains MIP-Authorization-  
2       Status set to False, then MIP6 service is not authorized for the subscriber. The HA SHALL construct a  
3       BA with status set to Administratively prohibited (129). The BA SHALL include the MN-HA AE  
4       which is signed by the MN-HA key received in the RADIUS Access-Accept packet or Diameter  
5       WHA6A command.
- 6       • If the HA receives the CUI attribute in the RADIUS Access-Accept packet or Diameter WHA6A  
7       command, it SHALL include it in all RADIUS/Diameter accounting packets only if it supports  
8       accounting message as indicated by the WiMAX-Capability attribute sent in the RADIUS Access-  
9       Request packet or Diameter WHA6R command, and if accounting messages were selected by the  
10      RADIUS/Diameter server in the WiMAX-Capability attribute. Similarly, if accounting is enabled and  
11      the Class attribute is received in the RADIUS Access-Accept packet/Diameter WHA6A command, the  
12      HA SHALL include the Class attribute in all accounting messages.
- 13     • If the HoA contained in the BU is unknown to the HA but the prefix of the HoA matches one of the  
14     prefixes that the HA supports for HoA construction, the HA will assume that the MS discovered the  
15     HL prefix info via bootstrapping. In this case, the HA may perform a local check in the local repository  
16     of Binding Cache Entries (BCEs) to make sure that the address (HoA) does not clash with that of  
17     another mobility binding. The HA SHALL perform the uniqueness validation of the assigned or  
18     requested HoA as per [57]. If the uniqueness of the HoA validation succeeds, the HA admits the  
19     binding and replies to the MS with a BA. The BA is protected by the MN-HA Mobility Message  
20     Authentication Option.
- 21     • If the HoA contained in the BU contains 0::0 (unspecified address) or EUI-64/IID the HA SHALL  
22     consider this as a request for a dynamic HoA assignment request from the MS. In the former case, the  
23     HA SHALL assign a 128-bit IPv6 address (HoA) from its local repository for the MS. In the latter  
24     case, the HA SHALL auto-configure a HoA with the received IID and a shared /64 prefix. In this  
25     document it is assumed that the /64 prefix is solely owned by the HA (i.e., no other HA owns and uses  
26     that prefix). HA SHALL make sure by checking in the local repository of BCEs that the auto-  
27     configured HoA does not clash with another HoA that is being used by some other user. If for some  
28     reason the HA finds a clash, the HA SHALL use either a globally unique /64 prefix to auto-configure  
29     the HoA or it SHALL use a shared /64 prefix to do the same. In the latter case, the HA SHALL again  
30     perform the BCE check to detect any clash. When the HA determines that the HoA assigned or auto-  
31     configured for the MS is unique, the HA SHALL admit the mobility binding for the MS with that  
32     HoA.
- 33     • If the HA receives Prepaid attributes/AVPs in the RADIUS Access-Accept packet or Diameter  
34     WHA6R command then it SHALL proceed to perform the prepaid procedures as specified in section  
35     4.4.3.3.
- 36     • If the HA receives Hot-lining attributes/AVPs in the RADIUS Access-Accept packet or Diameter  
37     WHA6R command then it SHALL proceed to perform the hot-lining procedures as specified in section  
38     4.4.3.5.
- 39     • If the HA supports accounting and the RADIUS/Diameter server requested accounting for this user,  
40     the HA SHALL send a RADIUS Accounting-Request Start with Session Begin set to TRUE or a  
41     Diameter ACR command with Accounting-Record-Type set to START\_RECORD as described in the  
42     Accounting session indicating that the Session has started.

43   Given the particular (HA) deployment assumptions for WiMAX Rel.1 the MS is always away from its home IP link  
44   and hence the HA is in a virtual home.

#### 45   **4.8.4.1.4   AAA Requirements and Behavior**

46   The HA interfaces with the HAAA server in the CSN.

47   During Device/User Network Access Authentication and Authorization procedures, the HAAA sends MIP6  
48   bootstrap information to the ASN (NAS and DHCPv6 Proxy) as specified in Section 4.1.

49   When the HA receives a BU from the MS, the HA constructs a RADIUS Access-Request packet or Diameter  
50   WHA6R command to fetch the MN-HA key which is needed for authenticating the BU. The RADIUS Access-  
51   Request packet is shown in Table 5-9. The Diameter WHA6R command is shown in Table 5-34.

1 During routing operations the VAAA SHALL process the NAI found in the User-Name attribute as specified by  
2 [68] and route the AAA messages accordingly. If VAAA chooses to send the AAA messages following the same  
3 route as taken by the network access authentication AAA messages, it MAY decorate the NAI with the decoration  
4 remembered from the network access authentication procedure.

5 The HAAA SHALL validate the Message-Authenticator in the RADIUS Access-Request packet as per procedures  
6 defined in [52]. If the message does not contain the Message Authenticator, or if the Message-Authenticator  
7 validation fails, then the HAAA SHALL silently discard the packet.

8 The User-Name AVP SHALL contain the Identity@realm that was used (pseudo or real) during Device/User  
9 Network Access Authentication and Authorization procedures. The AAA SHALL locate the Identity and ensure  
10 that it matches an internal identity. If PseudoIdentity was used and cannot be found, then the HAAA SHALL reply  
11 back with an RADIUS Access-Reject packet or Diameter WHA6R command with the error code indicating missing  
12 User-Name AVP.

13 If the pseudo Identity is found then the HAAA SHALL reply with a RADIUS Access-Accept packet as shown in  
14 *Table xx2* containing the MN-HA key encrypted using the procedures defined in [39] section 3.5 or Diameter  
15 WHA6R command containing the MN-HA key. The RADIUS packet SHALL include the Message-Authenticator  
16 computed according to [52].

17 If the HAAA determines that the user is not authorized for MIP6 then it SHALL set the value of the MIP-  
18 Authorization-Status to False. Otherwise if the user is authorized for MIP6 service, the HAAA SHALL set the MIP-  
19 Authorization-Status to True.

20 If the RADIUS Access-Request packet or Diameter WHA6R command contains the CUI attribute set to NULL, then  
21 the HAAA SHALL also include the CUI computed using the procedures defined in section 4.4.3 in the RADIUS  
22 Access-Accept packet or Diameter WHA6A command.

23 If the User is a prepaid user and prepaid is to be performed at the HA (providing the HA indicated it supports  
24 Prepaid Capabilities in the WiMAX-Capability Attribute/AVPs), then the HAAA SHALL include prepaid attributes  
25 in the RADIUS Access-Accept packet or Diameter WHA6A command as specified in section 4.4.3.3.

26 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  
27 supporting hot-lining as indicated in the WiMAX-Capabilities Attribute/AVP), then the HAAA SHALL include the  
28 hot-lining attributes as specified in section 4.4.3.5.

#### 29 **4.8.4.2 MIP6 Inter Access Router (AR) Handovers**

30 An ongoing session by an MS that is using CMIP6 may incur an inter Access Router handover. This may happen  
31 due to the MS incurring handover to a BS that has connectivity to a new Access Router or the serving ASN  
32 Functional Entity may decide to force a handover due to resource management reason or administrative reasons. The  
33 following sections detail the operation of such handovers.

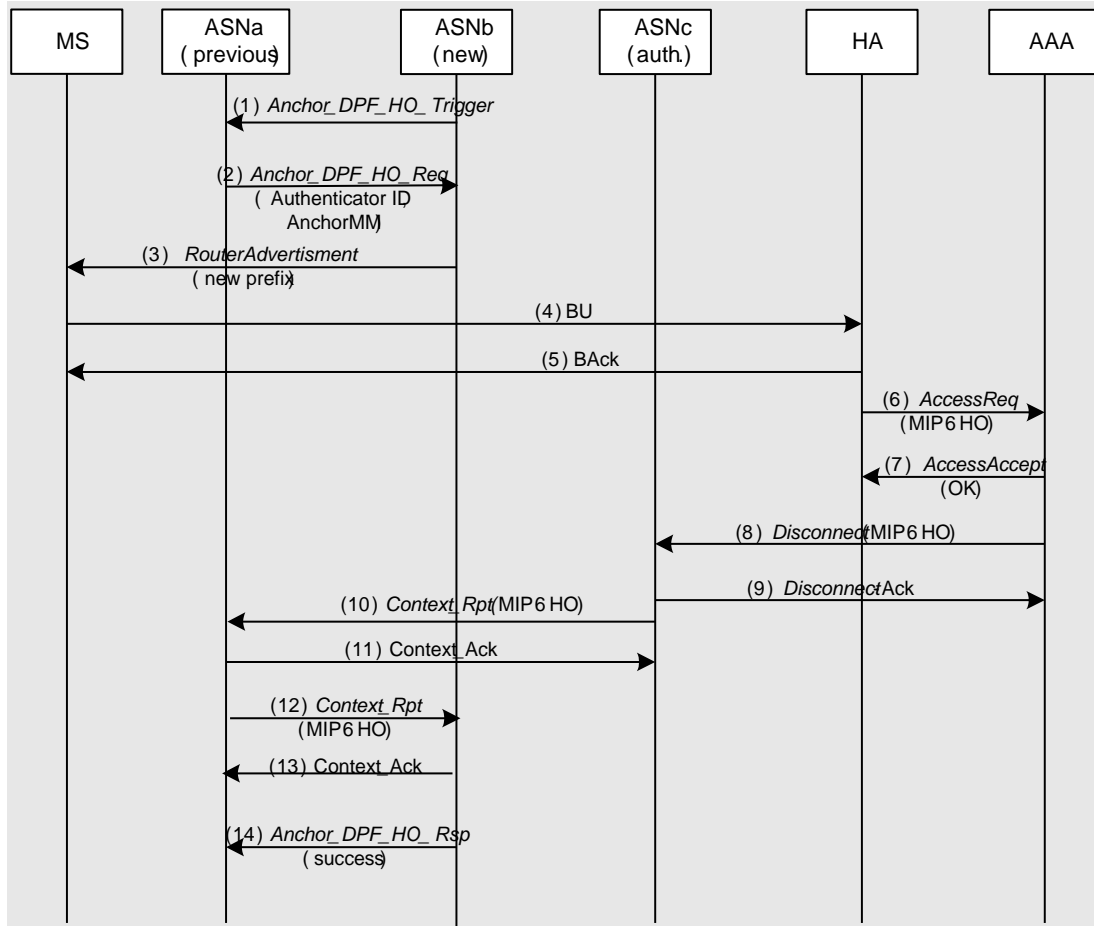


Figure 4-136 – CSN-Anchored Mobility Handover

### STEP 1

If the target ASNb initiates the anchor DPF relocation negotiation, it sends an *Anchor\_DPF\_HO\_Trigger* message to the anchor DPF in ASNa. If ASNa agrees with the anchor DPF relocation, it proceeds to Step 2. After sending *Anchor\_DPF\_HO\_Trigger*, ASNb starts the timer  $T_{\text{Anchor\_DPF\_HO\_Trigger}}$  for *Anchor\_DPF\_HO\_Req*. Once *Anchor\_DPF\_HO\_Req*, indicating the anchor DPF relocation decision of ASNa, is received by ASNb,  $T_{\text{Anchor\_DPF\_HO\_Trigger}}$  is stopped.

If the source ASNa initiates the anchor DPF relocation procedure, the call flow starts from Step 2.

### STEP 2

ASNa sends an *Anchor\_DPF\_HO\_Req* message to the DPF in ASNb. The message contains the authenticator address and the DHCP context information for the MS, and ASNa will start a timer  $T_{\text{Anchor\_DPF\_HO\_Req}}$  for *Anchor\_DPF\_HO\_Rsp* from ASNb.

### STEP 3

Target ASN for anchor DPF relocation sends a Router Advertisement message to the MS containing a new prefix used by the MS to formulate a new CoA.

### STEP 4

After the MS acquired the new CoA, it sends a MIP6 Binding Update (BU) message to the HA as per RFC 3375.



**STEP 5**

After receiving the Binding Update message, the HA updates its binding cache with the new CoA and responds to the MS with Binding Acknowledgment (BA) message indicating success.

**STEP 6**

After sending Binding Acknowledgment message, and if the newly registered CoA is different from the CoA that was in the HA's binding cache prior to registration, the HA send a RADIUS Access-Request packet or Diameter WHA6R command to the AAA server to inform it that the MS moved to a new location. Access-Request message contains a WiMAX specific VSA/AVP telling the AAA server that the message is sent with the purpose of informing the AAA that the MIP6 handover happened.

**STEP 7**

The AAA server confirms the receipt by sending a RADIUS Access-Accept packet or Diameter WHA6A command.

**STEP 8**

The AAA server sends a RADIUS Disconnect message or Diameter WASR command to authenticator to inform it that the MS successfully executed MIP6 handover procedure. Disconnect message/WASR command contains a WiMAX specific VSA/AVP telling the authenticator that the message is sent with the purpose of informing the ASN that the MIP6 handover happened.

**STEP 9**

The authenticator ASN acknowledges the receipt by sending a RADIUS Disconnect-Ack message or Diameter WASA command to the AAA server.

**STEP 10**

In response to Disconnect message/WASR command received in step 8, the authenticator ASN sends a Context\_Rpt message to the anchor DPF ASN. The Context\_Rpt message tells the ASNa that the MIP6 handover is successfully completed.

**STEP 11**

ASNa confirms the receipt of the Context\_rpt message.

**STEP 12**

The ASNa sends a Context\_Rpt message to the ASNb informing it that the MIP6 handover is completed.

**STEP 13**

ASNb confirms the receipt of the Context\_rpt message.

**STEP 14**

Triggered by the step 12, the target ASNb responds to the source ASNa with an *Anchor\_DPF\_HO\_Rsp* message indicating successful anchor DPF relocation. At this point the R4 tunnel between the ASNa and ASNb may be released and the previous anchor DPF may release any resources related to the MS.

**4.8.4.2.1 MS/ CMIP6 Client Operation**

The MS/ CMIP6 Client SHALL reset its MIP6 binding with a CoA as soon as the MS receives a new Router Advertisement from a new Access Router containing a prefix other than the one received in the router advertisement which was used for address autoconfiguration. This may either happen over an existing over-the-air link (resource management case) or it may happen due to change of the over-the-air link (handover). In either case, the MS SHALL perform IPv6 connectivity negotiation as defined in section 4.11.3. In case of stateful IPv6 address configuration scenario for CoA with DHCPv6, the MS won't be able to send and receive any data unless it

reconfigures the IPv6 stack with a new CoA via DHCPv6. This is because the target AR may not be able to support the CoA that the MS received while being served by the old AR. DHCPv6 based forced handover is not supported in this document.

Upon configuring a new CoA, the MS SHALL perform Mobile IPv6 BU/BA procedures. However, since it is an ongoing Mobile IPv6 session, the MS does not need to acquire the MIP6 bootstrap information from the target NAS. Also, the MS SHALL use the existing HoA and HA in the BU to update the CoA with the HA.

#### **4.8.4.2.2 AR/NAS and DHCPv6 Proxy Operation**

The target AR (target ASN) may receive *Anchor\_DPF\_HO\_Req* from an ASN Functional Entity to trigger a forced or regular handover.

Subsequently, the target AR SHALL send a RA to the MS to re-configure its CoA (if stateless auto-configuration of CoA is used in the ASN). It is assumed that the target AR has received the MIP6 bootstrap information from the Serving AR along with other state information via the context transfer procedure. The Target AR SHALL perform the same functions as described in section 5.6.3.1.2 to help the MS bootstrap the MIP6 parameters in case, the MS' DHCPv6 Client requests for such info.

Upon receiving a RADIUS Disconnect message/Diameter WASR command indicating successful completion of MIP6 handover, the authenticator SHALL send a Context\_Rpt message to the anchor DPF to inform it about the MS movement.

The serving AR SHALL receive a Context\_Rpt message from the authenticator indicating that MS completed the MIP6 handover. Upon receiving the Context\_Rpt message from authenticator, the serving AR SHALL inform the target AR of the successful MIP handover by sending a Context\_Rpt message to it.

Upon successful completion of MIP6 registration, the target AR SHALL send an *Anchor\_DPF\_HO\_Rsp* message to the ASN functional entity to complete the handover procedure and update the ASN functional entity with new mobility information.

After the CSN anchored handover is successfully completed the target AR function SHALL send the Context\_Rpt message to the anchor authenticator function. The Context\_Rpt message must contain the address of the new anchor DPF function. Upon receipt of the Context\_Rpt message containing the address of the new anchor DPF the authenticator must update its notion of the location of the anchor DPF function for this MS. The anchor authenticator SHALL confirm the receipt of the Context\_Rpt message by sending the Context\_Ack message.

After the CSN anchored handover is successfully completed the target AR function SHALL send the Context\_Rpt message to the serving BS. The Context\_Rpt message must contain the address of the new anchor DPF function. Upon receipt of the Context\_Rpt message containing the address of the new anchor DPF, the serving BS must update its notion of the location of the anchor DPF function for this MS. The serving BS SHALL confirm the receipt of the Context\_Rpt message by sending the Context\_Ack message.

#### **4.8.4.2.3 HA Behavior**

The HA SHALL process the BU from the MS with a new CoA when the associated mobility binding with the old CoA has not expired. The HA SHALL perform the BU validation as per section 5.6.3.1.3. If the BU processing is successful, the HA SHALL update the mobility binding with the new CoA information. Note that in this case, the HoA remains the same as the ongoing MIP6 session. The HA may adjust the MIP6 session lifetime to a different value (i.e., HA may consider this as a MIP6 session renewal) or the HA may respond back to the MS with remaining lifetime of the ongoing MIP6 session.

After updating the mobility binding for the MS and if the registered CoA was a new CoA, the HA SHALL send a RADIUS Access-Request packet or Diameter WHA6R command to the AAA server to inform it of the MS movement. The RADIUS Access-Request packet or Diameter WHA6R command SHALL contain a WiMAX-DM-Action-Code VSA/AVP indicating successful completion of MIP6 handover.

If the HA supports accounting and the RADIUS/Diameter server requested accounting for this user, the HA SHALL send a RADIUS Accounting-Request Stop with Session-Continue set to True followed by an RADIUS Accounting-Request Start Session Begin set to False indicating that the Session has started, as described in section 4.4.3.4.

#### 4.8.4.2.4 AAA Requirements

When the AAA server receives an Access-Request packet with a WiMAX-DM-Action-Code VSA indicating successful completion of MIP6 handover, it SHALL send a Disconnect message to the NAS to inform it of the MS movement. The Disconnect message SHALL contain a WiMAX-DM-Action-Code VSA indicating successful completion of MIP6 handover.

#### 4.8.4.3 MIP6 Session Renewal

The MIP6 MS performs Mobile IPv6 session renewal before expiry of the session lifetime if it wishes to continue the mobility session by sending a binding update to its HA.

##### 4.8.4.3.1 MS/ CMIP6 Client Requirements

The MS SHALL send a Binding Update to the HA if it wishes to continue the IPv6 mobility session. The MS SHALL construct the Binding Update as per the details described in 5.6.3.2.1.

##### 4.8.4.3.2 AR/ and DHCPv6 Proxy Requirements

The AR (ASN) has no requirements on session renewal.

##### 4.8.4.3.3 HA Requirements

The HA SHALL renew the mobility session upon successful processing of the Binding Update received from the MS before expiry of the mobility session lifetime. In response, the HA SHALL send back a BA to the MS following the procedure described in 5.6.3.2.3.

##### 4.8.4.3.4 AAA Requirements

None.

#### 4.8.4.4 MIP6 Session Termination

The IPv6 mobility session can be terminated as follows:

- a. By the MS by sending a Binding Update with lifetime set to 0.
- b. By the ASN functional entity upon detection of loss of radio link.

The following sections describe the requirements for each node for MIP6 session termination.

##### 4.8.4.4.1 MS/ CMIP6 Client Requirements

The MS SHALL send a BU to the HA with lifetime set to 0 if it wishes to terminate the IPv6 mobility session. The MS SHALL construct the BU as per the details described in 5.6.3.2.1. After receiving the corresponding BA, the MS SHALL tear down the IPv6 session if MIP6 was the only session for the MS.

##### 4.8.4.4.2 AR/NAS and DHCPv6 Proxy Requirements

Upon receiving a NetExit\_MS\_State\_Change\_Req from an ASN Functional Entity, the AR (the Serving DPF) SHALL initiate termination of the corresponding link (R6) for the MS. The AR (the serving DPF) may be able to inspect the BU/BAs that the MS exchanges with the HA.

In this case, the AR SHALL send a NetExit\_MS\_State\_Change\_Req to the ASN-functional entity and initiate teardown of 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 elapsed.

##### 4.8.4.4.3 HA Requirements

The HA SHALL teardown the mobility session upon successful processing of the BU received from the MS with lifetime = 0. In response, the HA SHALL send back a BA to the MS following the procedure described in 5.6.3.2.3. In the BA the HA SHALL set the lifetime to 0.

In the case of Diameter, the HA SHALL send a WSTR command to the HAAA indicating the termination of the mobility session.

If the HA supports accounting and the RADIUS/Diameter server requested accounting for this user, the HA SHALL send a RADIUS Accounting-Request Stop or Diameter ACR command with Accounting-Record-Type set to STOP\_RECORD with Session-Continue set to FALSE and Terminate-Cause set to User Request indicating that the Session has terminated and the MS left the network.

#### **4.8.4.4.4 AAA Requirements**

Upon receiving Accounting Request Stop for MIP6, the HAAA SHALL clear the MIP6 state of the user.

### **4.8.5 Proxy MIP6 R3 Mobility Management**

#### **4.8.5.1 PMIP6 Security**

There are two mandatory-to-implement and optional-to-use security mechanisms for PMIP6: One using [71] (i.e., in-band security), and the other not using any PMIP6-specific security but relying on the R3/R5 control plane security (i.e., lower-layer security). NSP and NAP decide which mode to operate based on their local policy and the dynamic negotiation during the network access authentication of the MS.

At least one of the lower-layer security or in-band security SHALL be used. Lower-layer security can be used if and only if R3 (and R5, when used) are secured (i.e., integrity and replay protected, data origin authenticated). In-band security SHALL be used in the absence of secure R3/R5.

Security mechanism is negotiated during the initial network entry of the MS using the RADIUS PMIP6-Service-Info VSA. Authenticator SHALL set bit #4 and bit #5 of the VSA value according to the availability of R3 security. These bits indicate ASN's capability. In-band Security bit (bit #5) is always set to 1, as [71] is mandatory to implement. Lower-layer Security bit (bit #4) is set to 1 if R3 security is present, 0 otherwise.

CSN that hosts the LMA SHOULD include PMIP6-Service-Info VSA in RADIUS Access-Accept packet. Only one of bits (bit #3 or bit #4) SHALL be set to 1 in the VSA and that bit indicates which security mechanism will be used for securing PMIP6 signaling for the MS. CSN SHALL set the Lower-layer Security bit to 1 only if R3 (and R5, when used) is secured and CSN prefers to use that mechanism. In all other cases, the In-band Security bit SHALL be set to 1. For example, CSN may require use of [71] even if R3/R5 is secured. In case the CSN does not support this dynamic negotiation mechanism (e.g., when core network residing in another IWK technology, such as 3GPP), PMIP6-Service-Info VSA MAY be missing in the CSN's RADIUS Access-Accept packet. Authenticator SHALL rely on R3/R5 security when that VSA is not provided by the CSN.

In case MS handovers from one ASN where R3 security is present to another ASN where it is not present, and the target ASN wants to initiate change of PMIP6 security mode, a re-authentication has to take place in order to change the negotiated security mechanism upon the handover. This change is feasible only to the LMA that supports the change of the security mechanism from in-band to lower-layer, or vice-versa, for the same MS upon an R3 handover.

When the negotiated mechanism is the lower-layer security, then the MAG/LMA SHALL not include Mobility Message Authentication Option [71] in the PBU/PBAs, and MAG/LMA SHALL drop any incoming PBU/PBA which carries that option.

The MN-NAI SHALL be set to PMIP-Authenticated-Network-Identity value when it is available to the MAG. In case it is not available, the MN-NAI SHALL be formulated using the username and the realm of the HCSN (if available) used in the EAP-Response Identity of the initial network access authentication.

VCSN that does not host the LMA SHALL not modify the content of the PMIP6-Service-Info VSA as it only proxies the AAA messages.

RFC 4285 [71] specification is originally written for RFC 3775 CMIP6 protocol [57]. Reference [71] also applies to PMIP6 [81] since PMIP6 is based on CMIP6. In order to apply [71] to PMIP6 (RFC5213) [81], a mapping profile is needed as the terminology in [71] is specific to CMIP6 [57]. Reference [71] SHALL be used in accordance with the following table as it gets implemented for securing PMIP6.

**Table 4-136 – Guidelines for using RFC 4285 for PMIP6**

RFC 4285 text	Usage guideline for PMIP6 implementation
Any text that refers to “MN”	Apply to the “MAG”
Any text that refers to “HA”	Apply to the “LMA”
Any text that refers to “BU”	Apply to “PBU”
Any text that refers to “BA”	Apply to “PBA”
MN-NAI Mobility Option [55]	If PMIP-Authenticated-Network-Identity is available, fill-in with this value. Otherwise, fill-in with the same username and home realm (if available) used in the EAP-Response Identity of the initial network access authentication.
“care-of address” value used in hash computation (Section 5.1 of [71])	Use the value of “PCoA” (MAG’s IPv6 address)
“home address” value used in hash computation (Section 5.1 of [71])	Use 128-bit value where prefix bits are set to “HNP” and suffix bits are set to 0.  When IPv4 address is allocated to the MS, the value is constructed using IPv4 MN-HoA in the upper 32 bits and lower 96 bits set to zero.

#### 4.8.5.2 Management of IPv6 and IPv4 support

The IPv4 and IPv6 mobility aspects of PMIP6 protocol are managed separately in WiMAX networks and can be authorized individually per subscriber or session basis by the HAAA server. The IPv4 support is an enhancement to PMIP6 protocol enabling mobility management of IPv4 hosts, as well as transport of payload over the IPv4 backhaul links. This specification distinguishes between IPv4 host mobility and transport capability in compliance with [93].

At the time of network access authentication, the indication and authorization of IPv6 and IPv4 support features are exchanged between the ASN and HCSN embedded in the dedicated AAA attribute:

- The ASN which is able to accommodate mobility management for IPv6 hosts SHALL indicate this capability setting bit #1 (Mobility support for IPv6) in PMIP6-Service-Info attribute of the RADIUS Access-Request. The ASN support of IPv4 hosts SHALL be indicated by setting bit #2 to value 1 (Mobility support for IPv4).
- If AR/MAG connects to the CSN via an IPv4 link then bit #3 (IPv4 transport backhaul support) in PMIP6-Service-Info attribute SHALL be set. In this case the AR/MAG must have another, IPv4 address assigned on its outbound interface. Bits #2 and #3 MAY be set simultaneously.
- When traversing over the VCSN which hosts the LMA, the VAAA MAY modify the contents of the Access-Request message to indicate IPv4 backhaul support is present. In this case VAAA SHALL append AAA attributes associated with the IPv4 support in PMIP6 such as information of the available DHCPv4 Server or the IPv4 address of the LMA in the VCSN.

Depending on the subscriber profile, network configuration policy, etc. the HAAA responds with RADIUS Access-Accept using the same bits in PMIP6-Service-Info attribute to authorize individual IPv6 and IPv4 support features.

- AAA response sent by the HAAA SHALL contain PMIP6-Service-Info attribute with bit #1 set when mobility for the host with an IPv6 address/prefix is authorized for a given subscriber and MAG.

- The AAA response SHALL include PMIP6-Service-Info attribute with bit #2 set when mobility for IPv4 host is explicitly authorized by the HAAA for the given subscriber/MAG.
- Bit #3 SHALL be set in AAA response when R3 reference point between MAG and LMA is IPv4-based (parameter is presumably deployment dependable where statically configured information may be available to the HAAA). The HAAA MUST provide the IPv4 LMA address in such response too.  
In this case both entities, MAG and LMA, utilize IPv4 addresses to communicate. Use of NAT on the IPv4 R3 path is allowed, where MAG can be using IPv4 address from the private range to establish the R3 transport tunnel.

In case IPv4 R3 link is available and authorized, MAG and LMA need to discover or mutually negotiate on the most suited transport mechanisms for the R3 path. Use of GRE tunnel may be dynamically negotiated as specified in [94] and Table 5-47, otherwise one of the IPv4 encapsulation modes specified in [93] must be used to convey IPv4 or IPv6 user payload over the R3.

Upon receiving a PBU with an IPv4 MAG source address, or a message attempting to register IPv4 HoA, the LMA SHOULD authorize such IPv4 support use in PMIP6 as part of the AAA query. In the Access-Request sent to the HAAA the LMA sets dedicated bit #2 (IPv4 host mobility SHALL be provided), and/or bit #3 (IPv4 R3 path SHALL be established) to identify the type of PMIP6 feature requested for the MS. If the requested PMIP6 feature is allowed, the HAAA sets the same bit to 1 in the Access-Accept, or value to 0 otherwise.

#### 4.8.5.3 PMIP6 Connection Setup Procedure

The PMIP6 connection setup SHALL take place after the initial network entry and access authentication is completed. The prerequisite for the procedure is the network's decision (derived by HCSN, or the ASN when multiple IP services are authorized by HAAA) to assign the network-based PMIP6 service for MS's IP session.

The AR/MAG MAY send the initial binding registration at any time following network authentication process. When multiple IP services are authorized, definition of decision- and trigger mechanisms that invoke PMIP6 binding registration is implementation specific.

The network authentication enables the ASN/NAS to negotiate and bootstrap the necessary PMIP6 mobility parameters and network configuration, including the assigned IP address or IPv6 prefix, security related settings, authorized address configuration mode(s), etc.

The connection setup procedures are differentiated by the address configuration process the MS undergoes. For an IPv6 MS the WiMAX network SHOULD provide both stateful and stateless address (auto)configuration modes with per-MS unique prefix assignment, while for IPv4 MS's PMIP6 procedure, the DHCPv4 support is needed to distribute the IPv4 MN-HoA to the MS.

##### 4.8.5.3.1 MS Requirements

The MS is not involved in PMIP6 mobility procedures and only required to perform the common address acquisition and configuration procedure to obtain IP mobility management via PMIP6.

An IPv6 MS SHALL act according to the information received from the AR/MAG in the (un)solicited Router Advertisement message. The address on MS's network interface is configured either by stateless address autoconfiguration or through stateful DHCPv6 configuration procedure following guidelines defined in section 4.11.4. The IPv6 address the MS configures for itself is in PMIP6 terms referred to as MN-HoA.

The IPv4 MS SHALL only use the DHCPv4 protocol to configure the IP address (IPv4 MN-HoA) that is served with network-based PMIP6 mobility management.

##### 4.8.5.3.2 AAA/NAS Requirements

The NAS and the HAAA engage in IP capability negotiation and service selection during the initial network entry. As part of the network authentication phase the PMIP6 capability indication SHALL take place between the ASN, the VCSN (if exists) and the HCSN:

- When PMIP6 support is available in the ASN, the NAS SHALL accordingly indicate MAG capability in the Access-Request sent to the AAA server (set bit #12 in ASN Network Service Capabilities TLV of WiMAX-Capability attribute). The NAS SHALL set bits for other IP Service Capabilities such as DHCPv4/v6 Proxy or Relay, when such functionalities are supported.

- 1 • The NAS SHALL explicitly inform the AAA of the IP transport and mobility abilities in scope of PMIP6 by  
2 including the indications in the PMIP6-Service-Info attribute: bit for lower-layer transport security is set (when  
3 such support is in place), mobility management for IPv4 and IPv6 hosts is indicated when supported by the ASN,  
4 and IPv4 backhaul support is indicated when present.
- 5 • When MS attaches through a visited network, the VCSN SHALL indicate its PMIP6 support, i.e., the LMA &  
6 DHCP capabilities, if those are available by adding the corresponding indications in the VCSN Network  
7 Capability TLV and other related attributes as part of the Access-Request message.
- 8 • If the HAAA acknowledges PMIP6 as an authorized IP service, it SHALL deliver the related PMIP6  
9 subscriber/service profile information in the AAA Access-Accept message sent to the ASN and VCSN. The  
10 profile MUST provide the following information:
  - 11 - PMIP6 listed under Authorized IP Network or Visited Authorized Network Services.
  - 12 - Address of the home- and/or visited LMA designated for that specific MS's IP session. When IPv4  
13 transport is to be used over R3, the IPv4 address of the home- or visited-LMA has to be present.
  - 14 - If available at the HAAA, the IPv6 Home Network Prefix (HNP) or the IPv4 MN-HoA. Both configuration  
15 options may be present in the HAAA response.
  - 16 - When DHCP service for PMIP6 is authorized, information associated with the DHCP Proxy/Relay  
17 functions e.g., the DHCPv4/v6 server address, DHCP security parameters, etc.
  - 18 - Authorization of host IP mobility type (IPv6 and/or IPv4 bit SHALL be set in responding the PMIP6-  
19 Service-Info attribute)
  - 20 - Directive on PMIP6 signaling protection method to be applied (lower-layer or in-band protocol security  
21 bits in the PMIP6-Service-Info attribute)
  - 22 - Security bootstrapping parameters (PMIP6 root key and the associated SPI)
- 23 • The NAS/Authenticator SHALL store the obtained information locally and keep it available to the corresponding  
24 PMIP6 mobility entities in the ASN (MAG, DHCP function, etc.) throughout the IP session lifetime.

25 During routing operations the VAAA SHALL process the NAI found in the User-Name attribute as specified by  
26 [68] and route the AAA messages accordingly. If VAAA chooses to send the AAA messages following the same  
27 route as taken by the network access authentication AAA messages, it MAY decorate the NAI with the decoration  
28 remembered from the network access authentication procedure.

#### 29 **4.8.5.3.3 AR/MAG Requirements**

30 The AR/MAG MUST obtain the Home Network Prefix (or IPv4 Home Address) before sending the first Router  
31 Advertisement or proceeding with DHCP message exchange. The means to allocate HNP/HoA include  
32 bootstrapping from the AAA server, or assignment by the LMA via PBU-PBA exchange.

33 The PMIP6 IP mobility management for the attaching MS is authorized on per-MS basis by the HAAA appending  
34 the appropriate authorization hint in the Access-Accepts PMIP6-Service-Info attribute. Bit #1 is set if assignment  
35 and mobility of IPv6 address/prefix is authorized for the MS, bit #2 is set when mobility with an IPv4 address is  
36 allowed. The AR/MAG SHALL act corresponding to the mobility type authorization when constructing the PBU  
37 message: if both mobility types are authorized, the PBU SHOULD include both HNP and IPv4 Home Address  
38 mobility options. For constructing the PBU and processing PBA response from the LMA, the AR/MAG SHALL  
39 follow requirements from [81] on MS attachment and initial binding registration, and receiving the PBA, with one  
40 key difference. Inline with PMIP6 service authorization results from the Access-Accept, the AR/MAG MUST apply  
41 in-band protocol security to the PBU sent to the LMA. When lower-layer transport security is only requested by the  
42 HCSN, AR/MAG will abandon explicit protection of PMIP6 control plane.

43 The initial PBU SHALL be formed in accordance with guidelines in section 5.7, and needs to contain valid MN  
44 identifier information, HO indicator option with value set to attach over a new interface (HOI=1), the Access  
45 Technology Type (ATT) option with value set to 5 to indicate WiMAX access, the link-local address option, and the  
46 Timestamp mobility option. The HNP and IPv4 HoA mobility options will be populated in the PBU if the  
47 information was obtained prior from the AAA server. The remaining PBU fields and mobility options are composed  
48 as defined in Table 5-47.

When IPv4 support in PMIP6 is utilized, the AR/MAG SHALL operate as specified in [81]. If the R3 reference point is completely IPv4-based, the AR/MAG SHOULD register an IPv4 Proxy CoA in the BCE at the LMA being the source IP address of the outer IPv4 packet encapsulating the PBU.

The AR/MAG MAY send the initial binding registration at any time following network authentication process. When multiple IP services are authorized specification of decision- and trigger mechanisms that invoke AR/MAG to send the initial binding registration is implementation specific.

Based on indication received in AAA Access-Accept or from local configuration, the AR/MAG decides on address configuration mode to be applied for the MS's PMIP6 session. When DHCPv6 configuration mode is authorized (appropriate DHCP attribute(s) present in the Access-Accept) the AR/MAG SHALL correspondingly assign either the DHCPv6 relay function or DHCPv6 proxy function for this IP session. The AR/MAG MUST set related address configuration flags in the (un)solicit RA sent to the MS corresponding to the address configuration mode associated with the MS's IP session; "A" flag is set in the Prefix Information Option if the MS is allowed to autoconfigure the address from the HNP contained within, otherwise the "M"/"O" RA flags MUST be set.

The common link-local addresses that AR/MAG has to use on the interface towards the MS SHOULD be coordinated and distributed by the LMA enclosed in the specific PMIP6 mobility options (Link-local address, and IPv4 default-router options) unless statically preconfigured to the same value on all MAGs in the domain. Initial AR/MAG SHALL include the Link-local Address option set to ALL\_ZERO when performing the initial registration to request the LMA to generate a valid LLA value. The dynamic approach helps better in scaling the PMIP6 domain as it makes the necessary information directly available for the target MAG in all successive handover occurrences within the domain.

#### 4.8.5.3.4 DHCP Proxy/Relay Requirements

Choice of IP address configuration mode is based on Access-Accept received from the HCSN as a result of the WiMAX ASN/CSN capability negotiation and subscriber/network authentication procedure. As described in section 4.4.1.6.3, provision of home- or visited DHCPv6 server address in subscriber profile information from the AAA indicates authorization of DHCPv6 Relay mode. Lack of DHCP server information in AAA response implies use of the Proxy mode. When DHCP Proxy configuration is pre-provisioned by the AAA server, inclusion of HNP and Interface ID parameters is needed to allow generation of the full IPv6 HoA/128.

General requirements on DHCPv6 operation with respect to Proxy and Relay mode apply here, as specified in section 4.13.5.2 respectively.

When PMIP6 with IPv4 support service is assigned to the MS, the requirements for DHCPv4 Proxy (section 4.8.2.1.2.1) and DHCPv4 Relay (section 4.8.2.1.2.2) apply likewise.

The DHCP entity learns the MS's addressing information (HNP or IPv4 MN-HoA) either from the NAS or the AR/MAG. The NAS SHALL provide the HNP/MN-HoA to the DHCP function only when such information is received directly from the HAAA. Otherwise the AR/MAG will deliver the HNP/HoA after the LMA has allocated and verified the prefix/address.

The DHCP entity in the ASN MUST delay responding to all DHCP requests (DHCPv6 Solicit, DHCPv4 Discover, etc.) until the initial binding registration for the MS is completed and BCE established. When forwarding the DHCP Solicit/Discover or Request messages to the DHCP Server, the DHCP Relay in the ASN MUST include the HNP/IPv4 MN-HoA already associated with the MS as a hint for the DHCP Server.

#### 4.8.5.3.5 LMA Requirements

The LMA SHALL support relevant PMIP6 AAA attributes defined in section 5.4.2 needed for wholesome IP service bootstrapping, authorization and key derivation when in-band security is used.

The LMA processing of received PBUs and creation of PBA responses, BCE population and routing management SHALL follow requirements from [81]. The PBA message sent in response to the initial PBU SHALL contain a valid MN ID option, HO indicator option with value set to 1, Access Technology Type set to value 5, populated link-local address option if one was present in the PBU, and the Timestamp option. The remaining PBA fields and mobility options are composed as defined in Table 5-47.

The LMA SHALL support in-band protocol security as described in section 4.8.5.1. The received PBU that entails signaling protection in form of valid authentication option MUST be replied a PBA using the same protection



mechanism. The PBUs received without embedded signaling protection SHALL be processed and acknowledged only if the source MAG is considered trusted and use of Authentication Options (AO) is not enforced for that PMIP6 peer. When enabling the in-band signaling protection the LMA SHALL participate in the PMIP6 key derivation and management process as specified in section 4.3.5.3.4.

When IPv4 support in PMIP6 is utilized, the LMA MUST operate as specified in [81]. If the R3 reference point is completely IPv4-based, the LMA MUST accept registration of IPv4 Proxy CoA to MS's BCE. The LMA SHOULD verify the PMIP6 mobility management for the attaching IPv4 MS is permitted at the time of processing the initial PBU through the AAA query.

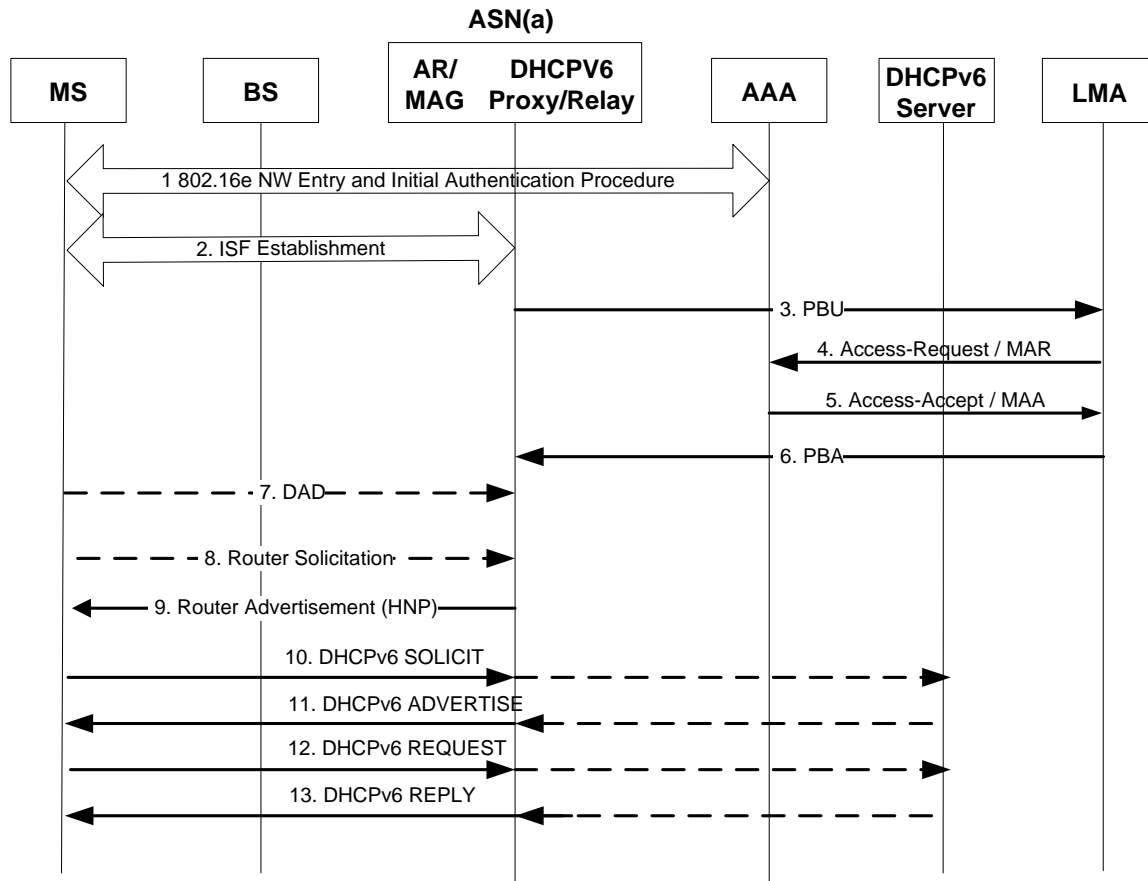
Depending on the parameters provided by the AR/MAG in the PBU, LMA provides different operation modes.

- In the case the PBU includes the HNP and/or IPv4 MN-HoA information, the LMA verifies that the MS is eligible for the allocated address e.g., against the AAA or DHCP server, and creates the BCE that binds the location of the MS with the MN ID and HNP/HoA it received. The LMA SHALL allow simultaneous registration of IPv4 MN-HoA and HNP for the MS when obtained from a single PBU message.
- In case AR/MAG does not include valid information option but the mobility option with ALL\_ZERO value, the LMA MUST allocate HNP and/or MN-HoA, assigns the information to the MS, accordingly records it in the BCE, and finally provides the information to the AR/MAG enclosed in the Proxy Binding Acknowledge message. For this purpose the LMA MAY interwork with a (non)collocated DHCP server.
- The LMA SHALL perform a determination process for PMIP6 tunnel method: if the PBU is received with an IPv4 Proxy-CoA, the LMA MUST invoke creation of the IPv4 bi-directional PMIP6 tunnel over the R3 for that specific MS. If a GRE Key option [94] was included in the PBU, the LMA that supports the GRE encapsulation over R3 SHOULD meet the request for GRE key exchange from the AR/MAG and thus SHOULD provide the uplink key in the PBA.
- The LMA SHALL manage the AR/MAG link-local address (LLA) unless the LLA parameter is not statically and identically configured on all MAGs across the PMIP6 domain. If the LLA mobility option (with ALL\_ZERO value) is received as part of the initial PBU, the LMA SHALL generate , store and confirm the appropriate value in the responding PBA to be used in all subsequent HO events while this IP session lasts.

#### **4.8.5.3.6 PMIP6 Connection Setup flows**

##### **4.8.5.3.6.1 Stateful DHCPv6 connection setup**

Figure 4-137 presents PMIP6 connection setup procedure through stateful DHCPv6 address configuration according to the MS profile information retrieved from the AAA. The call-flow is equally applicable for use of both DHCPv6 Proxy and DHCPv6 Relay functions in the ASN.



**Figure 4-137 - PMIPv6 connection setup procedure through DHCPv6**

#### STEP 1

MS performs 802.16e network entry procedure and initiates WiMAX authentication with AAA. During initial authentication phase the AAA downloads the subscriber profile to the ASN/ASN-GW, which contains the LMA IP address and may contain HNP information and address of the DHCPv6 server.

#### STEP 2

After successful WiMAX authentication and registration, the SFA in ASN (a) initiates ISF establishment using the link local address of the MS.

#### STEP 3

The AR/MAG in ASN (a) sends a PBU message to the LMA's IP address received in the AAA response. The PBU message composition is presented in section 4.8.5.3.3. If the HNP was obtained from the HAAA, this information populates the Home Network Prefix option included in the PBU.

The PBU/PBA, the DAD (step 7) and Router Solicitation RS (step 8) are independent procedures and may occur at any given time after the Initial authentication/authorization (Step 1) and (for DAD and RS) after ISF establishment (Step 2).

**STEP 4**

After receiving the PBU message (message composition in section 4.8.5.3.3), the LMA initiates Authorization of MAG ASN(a) that has sent the Proxy Binding Update by sending either RADIUS Access-Request or Diameter MAR message to the AAA. When in-band security is enabled, if needed the LMA will also retrieve the necessary keying information from the AAA.

**STEP 5**

The AAA responds with either RADIUS Access-Accept or Diameter MAA message to the LMA and thereby assigns and acknowledges the HNP to be used for the MS's PMIP6 session. LMA creates a tunnel towards the AR/MAG ASN (a) and sets the routing rule directing all packets destined to the HNP via the established PMIP6 tunnel.

**STEP 6**

The LMA sends the PBA to the AR/MAG ASN (a) to confirm the initial binding registration and invokes creation of the dynamic bi-directional PMIP6 tunnel for MS's uplink and downlink payload forwarding. The PBA includes the MS's assigned prefix in the HNP option, has the HO indicator value set to one, the ATT option set to value five, and the Link-local option populated as described in section 4.8.5.3.5.

**STEP 7**

Triggered by the establishment of the IPv6 ISF, the MS configures a link local address, and MAY start a duplicate address detection process to verify it.

**STEP 8**

MS MAY send a Router Solicitation message in attempt to learn the available routers on the link.

**STEP 9**

AR/MAG ASN(a) sends the IPv6 Router Advertisement message with the HNP information enclosed in the Prefix information option (the "A" flag may not be set). If the AAA response and local policy allows for DHCPv6-based address configuration, the RA sets the Managed Flag to 1.

**STEP 10**

- In the case that Managed Flag is set to 1 in the Router Advertisement message, MS initiates the DHCPv6 procedure by invoking the DHCPv6 client to send DHCPv6 Solicit message to the DHCP entity collocated with the AR/MAG.
- In case DHCPv6 server address was present in the AAA response, ASN MAY provide address configuration through the DHCP Relay function. Otherwise the ASN(a) provides the DHCP Proxy based address configuration.
- In case of a DHCPv6 Relay, the DHCPv6 Relay ASN (a) forwards the DHCPv6 Solicit message to the assigned DHCPv6 server. The message must include the HNP associated with the MS as a hint to the server.

**STEP 11**

- In the DHCPv6 Proxy case, the DHCPv6 Proxy in ASN (a) allocates the IPv6 HoA from the already known HNP and sends the DHCPv6 advertisement message to the MS.
- In the case of a DHCPv6 Relay, the DHCPv6 Relay in ASN (a) receives DHCPv6 Advertisement message from the DHCPv6 server and sends a DHCPv6 Advertisement message to the MS.

**STEP 12**

The MS sends a DHCPv6 Request message to ASN (a)

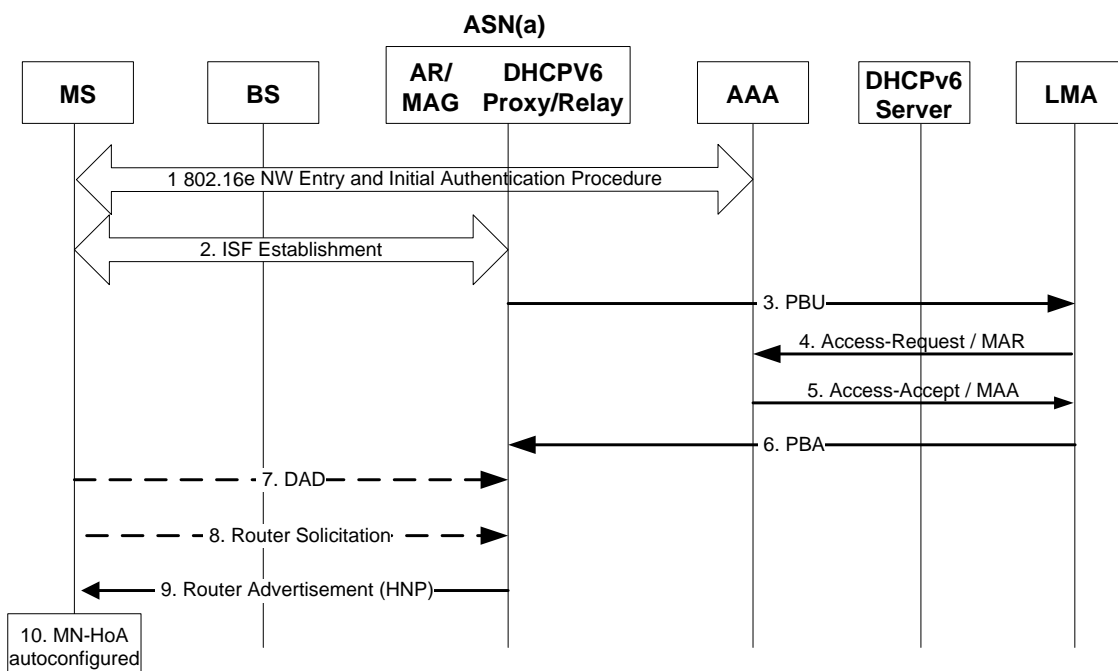
- In case of a DHCPv6 Relay, the DHCPv6 Relay in ASN (a) forwards the DHCPv6 Request message to the DHCPv6 server. The message includes the HNP associated with the MS as a hint to the server.

### STEP 13

- In the case of a DHCPv6 Proxy, the DHCPv6 Proxy in ASN (a) responds to the MS's request by sending the DHCPv6 response message containing the assigned MN-HoA/128.
  - In the case of a DHCPv6 Relay, the DHCPv6 Relay in ASN (a) obtains the response from the server containing the assigned MN-HoA/128 and sends the DHCPv6 response message further to the MS.
- After this step the MS MAY initiate request for an IPv4 HoA assignment if such service is authorized and supported by the network.

#### 4.8.5.3.6.2 Stateless address autoconfiguration connection setup

Figure 4-138 presents PMIP6 connection setup based on IPv6 stateless address autoconfiguration procedure.



**Figure 4-138 - PMIP6 connection setup procedure with SLAAC**

### STEP 1

MS performs 802.16e network entry procedure and initiates WiMAX authentication with the AAA. During initial authentication phase, the AAA downloaded subscriber profile to the ASN-GW/ASN; including the address of the LMA and the Home Prefix (e.g. it is an option).

### STEP 2

After successful WiMAX authentication and registration, the SFA in ASN (a) initiates ISF establishment using the link local address of the MS.

### STEP 3

The AR/MAG ASN (a) sends a PBU message (description in section 4.8.5.3.3) to the LMA that is specified in the MS profile obtained from the AAA. If Home Network Prefix exists in the subscriber profile, the populated Home Network Prefix Option is included in the PBU message.

[Note: PBU/PBA, DAD, RS are independent procedures and may occur at any given time after the network authentication/authorization.]

**STEP 4**

After receiving a PBU message, the LMA initiates Authorization of AR/MAG ASN (a) that has sent the PBU by sending either RADIUS Access-Request packet or Diameter MAR message to the AAA.

**STEP 5**

The AAA responds with RADIUS Access-Accept packet or Diameter MAA message to the LMA which updates the location of the MS and creates a tunnel between the AR/MAG in ASN(a) and LMA in order for all the packets destined to Home Network (Prefix) associated with the MS to be routed to the newly created tunnel.

**STEP 6**

The LMA sends a PBA message (description given in section 4.8.5.3.5) to the AR/MAG ASN (a) which then creates a tunnel with the MAG.

**STEP 7**

Triggered by the establishment of the IPv6 ISF, the MS configures the link local address, and may start the duplicate address detection process.

**STEP 8**

MS may send a Router Solicitation message to learn the available routers on the link.

**STEP 9**

The AR sends a Router Advertisement message to the MS. The Router Advertisement message with the “A” flag set contains per-MS unique prefix HNP/64 which allows the MS to directly autoconfigure its PMIPv6 MN-HoA.

**STEP 10**

The MS configures a globally routable IPv6 address using the stateless autoconfiguration process. The MS MAY trigger the duplicate address detection (DAD) for the IPv6 address it has autoconfigured on the network interface to verify its uniqueness on the link.

After this step the MS MAY initiate request for an IPv4 HoA assignment if such service is authorized and supported by the network.

### 4.8.5.3.6.3 Connection setup for IPv4

Figure 4-139 shows the connection setup procedure via PMIP6 for an IPv4 MS:

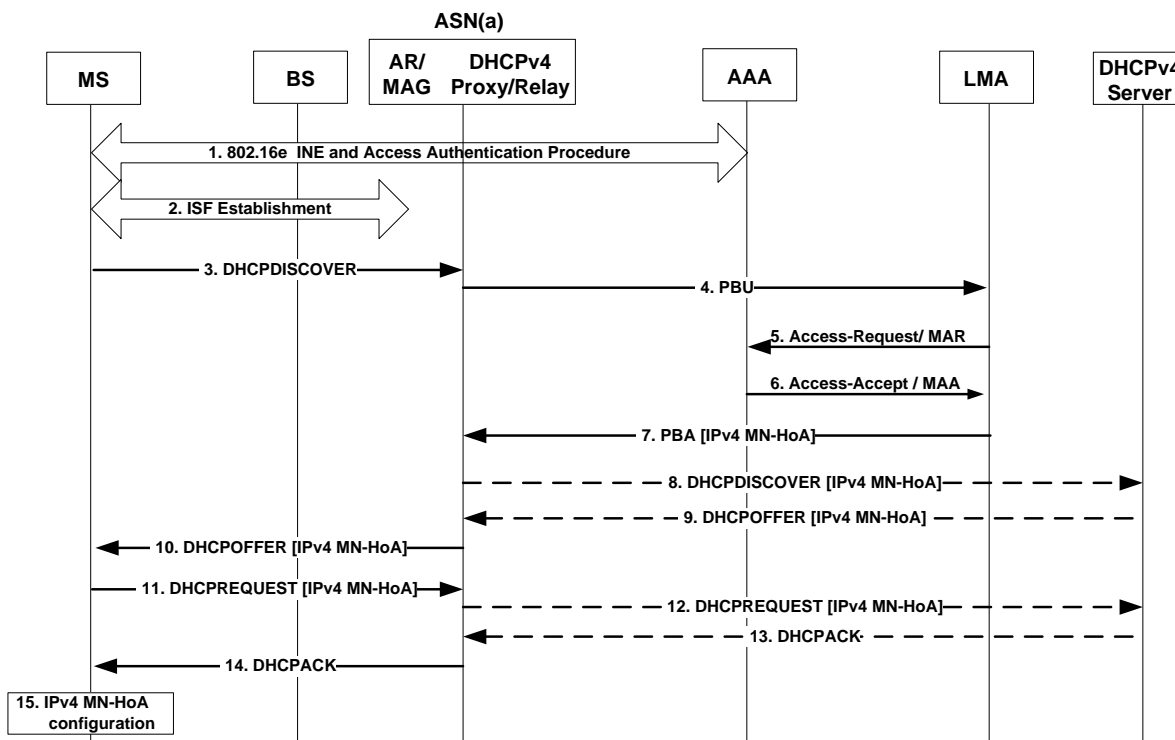


Figure 4-139 - PMIP6 Connection Setup for an IPv4 MS

#### STEP 1

MS performs 802.16e network entry procedure and initiates WiMAX authentication with AAA. During initial authentication phase, the AAA downloads subscriber profile to the ASN-GW/ASN; it may include the LMA address and the IPv4 Home Address (IPv4 MN-HoA).

#### STEP 2

After successful WiMAX authentication and registration, the SFA ASN(a) initiates ISF establishment.

#### STEP 3

MS sends DHCPDISCOVER message in attempt to configure the IPv4 address on its network interface.

#### STEP 4

The AR/MAG ASN (a) sends a PBU message (described in section 4.8.5.5.3) to the LMA designated for the attaching MS. If IPv4 MN-HoA was provided in the MS profile, the populated IPv4 Home Address option is included in the PBU message.

[Note: PBU/PBA and DHCPDISCOVER messages are independent procedures and may occur at any given time after the network authentication/authorization.]

#### STEP 5–6

LMA initiates Authorization of AR/MAG ASN (a) that has sent PBU and sends either RADIUS Access-Request packet or Diameter MAR message to the AAA. Upon receiving the AAA response (RADIUS Access-Accept or Diameter MAA message) the LMA updates the BCE and creates a transport tunnel towards the MAG in ASN (a).

**STEP 7**

The LMA sends a PBA message (described in section 4.8.5.3.5) to the AR/MAG in ASN (a) including the authorized or self-allocated IPv4 MN-HoA. The MAG completes setting up the transport tunnel over the R3.

**STEP 8-9**

These are optional steps, applicable only when address allocation takes place over the DHCP Relay. The ASN (a) forwards the DHCPDISCOVER towards the designated DHCP Server, including the IPv4 MN-HoA address received previously in the PBA message. DHCP Server responds with the DHCPOFFER message.

**STEP 10 –15**

MS completes the DHCPv4 procedure configuring the previously offered IPv4 MN-HoA address. In case of a DHCP Relay, the DHCPREQUEST and DHCPACK messages will be routed through ASN(a) on the path to/from the associated DHCP Server.

After this step the MS MAY initiate request for an IPv6 HNP assignment if such service is authorized and supported by the network.

**4.8.5.4 PMIP6 Session Renewal Procedure**

**4.8.5.4.1 DHCP Renewal**

In the case that the global address was initially configured with DHCPv6, the MS and ASN SHALL support procedures for lease extension as per RFC 3315 [47].

In the case the global MN-HoA or IPv4 MN-HoA address was initially configured though DHCPv6 or DHCPv4, the associated DHCP entity in the ASN SHOULD assure the assigned address/prefix lease time is less or equal to the PMIP6 binding lifetime.

**4.8.5.4.2 PMIP6 Lifetime Renewal**

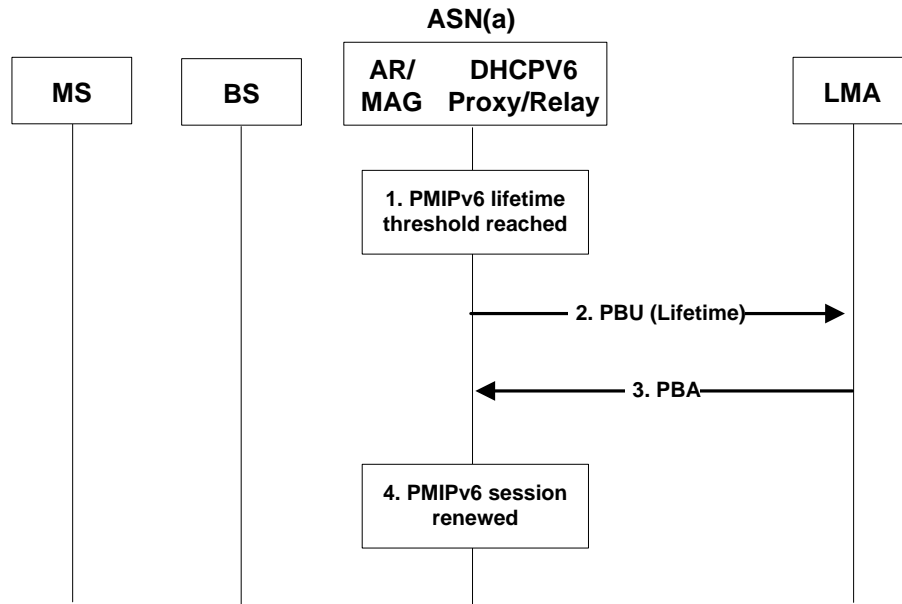
Session renewal in the case of PMIP6 service is about extending both the address lifetime of the MS and PMIP6 session lifetime of the LMA.

In case a stateless address autoconfiguration was used to configure the global address, the MS and ASN SHALL support mechanisms defined in [78] for extending the lifetime of the autoconfigured address.

As for extending the lifetime of a currently existing binding at the LMA, the AR/MAG ASN (a) MUST send a Proxy Binding Update message with the Handoff indicator option set to value of 5 (Re-registration) and a new specific lifetime.

Upon accepting the PBU request for extending the lifetime of a currently active binding, the LMA MUST update the lifetime for that binding and send a PBA message to the MAG ASN(a).

Figure 4-140 presents PMIP6 session renewal procedure by MAG ASN (a) triggering.



**Figure 4-140 - PMIPv6 Lifetime Renewal**

#### STEP 1

The MAG in ASN (a) determines that the remaining lifetime of a particular PMIPv6 session has reached a threshold.

#### STEP 2

The MAG ASN (a) sends a Proxy Binding Update message with a new proposed lifetime value to the LMA to extend the PMIPv6 session. The PBU includes Handoff Indicator option with the value set to 5 (HO state not changed), and the HNP assigned to the MS.

#### STEP 3

The LMA renews the lifetime of a particular PMIPv6 session and MS's BCE, and sends a responding Proxy Binding Acknowledgement to the AR/MAG in ASN(a).

#### STEP 4

The MAG in ASN (a) receives a Proxy Binding Acknowledgement message and extends the lifetime of the MS's PMIPv6 binding and the IP session.

### 4.8.5.5 PMIPv6 CSN Anchored Mobility Handover

#### 4.8.5.5.1 MS Requirements

There are no specific requirements towards the MS for the case of PMIPv6 handover. The new serving ASN(b) SHOULD assure the appropriate link configuration and the same address of the first-hop AR/MAG get consistently advertised to the MS after the HO, to hide the actual change of the attaching link.

When MS receives the Router Advertisement message from the new serving AR/MAG containing the same HNP information, it SHOULD retain both, the configured HoA and Home Network Prefix on its network interface without any change.

#### 4.8.5.5.2 Authenticator and AAA Server Requirements

Until re-authentication or Authenticator relocation takes place, the anchor Authenticator MUST maintain the security context associated with the specific MS throughout the IP session lifetime.



Upon receiving *Anchor\_DPF\_Relocate\_Req* message from a Target ASN(b) indicating an Anchor DPF relocation request, the Anchor Authenticator may use a local policy to determine whether the relocation is allowed or not. If relocation is allowed, the Anchor Authenticator responds with an *Anchor\_DPF\_Relocate\_Rsp* message that includes a success code. If the PMIP6 session requires in-band protocol security (use of AO in the PBU and PBA), the Anchor Authenticator SHALL derive and provide the required security material (MAG-LMA-PMIP6-Key, associated SPI, and lifetime) valid for the specific MAG, LMA and the MS triplet in the *Anchor\_DPF\_Relocate\_Rsp* message.

If the Anchor Authenticator determines that the Anchor DPF relocation is not allowed (for example, Authenticator relocation must happen before Anchor DPF relocation or relocation not allowed on account of the local policy), the Anchor Authenticator SHALL reject the relocation request by sending *Anchor\_DPF\_Relocate\_Rsp* message with the appropriate reject code (Result Code TLV with error code = 0x02, Failure – Not supported).

If the PBU registration is successful with the new MAG at the Target ASN(b), the Anchor Authenticator SHALL update the Anchor DPF (new MAG) location information upon receiving the *Anchor\_DPF\_Relocate\_Ack* message with a success indication from the Target ASN(b).

The AAA server SHALL provide the relevant PMIP6 service authorization (and the PMIP6-RK key if in-band protocol is required) to the LMA when the Access-Accept request is sent as a result of receiving the PBU from the new target AR/MAG. When in-band security is used, and if the LMA has a valid PMIP6-RK key, it MAY abandon the AAA query and reuse the PMIP6-RK key to derive the new MAG-LMA-PMIP6 key for the location registration from the target AR/MAG.

#### 4.8.5.5.3 AR/MAG Requirements

A PMIP6 CSN Anchored Mobility Handover is usually initiated in a situation where Data Path for the MS has already been established at the new serving ASN(b). In case of idle mode the data path is not present when HO is initiated. The key triggers for initiating the PMIP6 handover procedure are:

- Resource management and optimization decision by the network
- Idle mode location update from a new serving ASN.

When the MS has established the data path on the new serving ASN(b), triggered by one of the HO events, the new serving ASN(b) MAY initiate PMIP6 HO by sending the *Anchor\_DPF\_HO\_Trigger* message to the anchor ASN(a) for PULL handover mode. The trigger message is formed as defined by Table 4-114. The anchor ASN(a) either responds or self-initiates the handover (PUSH mode) by sending the *Anchor\_DPF\_HO\_Req* to the serving ASN(b). The message contains the relevant information associated with the specific PMIP6 session; allocated HNP or IPv4 HoA, LMA IP address, protocol configuration details such as DHCP- and security mode (if applicable), etc. The *Anchor\_DPF\_HO\_Req* message definition is provided in Table 4-138.

The target ASN(b) SHALL send an *Anchor\_DPF\_Relocate\_Req* message to the anchor Authenticator requesting a PMIP6 HO. If the ongoing PMIP6 session requires in-band protocol security (use of AO in the PBU/PBA), the target ASN(b) SHALL request the keying information from the anchor Authenticator needed to protect the forthcoming PMIP6 signaling exchange with the LMA.

In case that target AR/MAG in ASN(b) receives *Anchor\_DPF\_Relocate\_Rsp* (defined in Table 4-139) message from the anchor Authenticator, it SHALL trigger PBU/PBA procedure to register MS's new location and create the PMIP6 tunnel between itself and the LMA. If the PBU registration procedure is successful, the Target ASN(b) SHALL update the anchor Authenticator with the new AR/MAG location by sending the *Anchor\_DPF\_Relocate\_Ack* message with a success code, otherwise a failure code indicating unsuccessful PBU registration is sent. The Target ASN(b) SHALL also inform ASN(a) of the PBU registration result by sending an *Anchor\_DPF\_HO\_Rsp* with an appropriate result code (Result Code TLV with error code = 0x02, Failure – Not supported).

If the Target ASN(b) receives an *Anchor\_DPF\_Relocate\_Rsp* message indicating a reject code by Anchor Authenticator, the Target ASN(b) SHALL inform ASN(a) about the rejected Anchor DPF relocation by sending an *Anchor\_DPF\_HO\_Rsp* with an appropriate reject code.

In case the serving AR/MAG in ASN(a) receives the *Anchor\_DPF\_HO\_Rsp* message indicating a successful DPF relocation, it SHALL release the resources allocated for the given MS, local mobility context and bindings, the R4

data path, as well as the PMIP6 tunnel towards the LMA. The *Anchor\_DPF\_HO\_Rsp* is formed as defined in Table 4-115. Otherwise, it continues to anchor the DPF and acts as the AR/MAG for the MS.

The Target AR/MAG SHALL perform the PBU registration procedure following the guidelines specified in [81] (and [93] for PMIP6 with IPv4 support). The PBU MUST contain the MN ID, HNP or IPv4 HoA option (or both, if obtained in PMIP6 mobility context from the previous MAG), the Access Technology Type (set to value 5 for WiMAX), the Handoff Indicator option (set to value of 3, handoff between mobile access gateways for the same interface), and the Timestamp option. When the Link-local Address is not statically preconfigured, the LLA option (set to value ALL\_ZERO SHALL be included in the PBU to request the LMA to provide the current in-use AR downlink address. The remaining PBU fields and mobility options are composed as defined in Table 5-47.

Upon receiving PBA from the LMA indicating registration success, the new AR/MAG in ASN(b) updates its local MS context and mobility binding with the information obtained, creates PMIP6 transport tunnel towards the LMA and installs the needed forwarding rules.

In all subsequent communication with the MS, the new AR/MAG MUST configure and use the interface and link parameters according to information received from the previous AR/MAG and the LMA (advertisement of the HNP, Link-local and DHCP address, etc.).

#### 4.8.5.5.4 LMA Requirements

The LMA SHALL support the PMIP6 service authorization and negotiation extensions against the AAA server by supporting the specific AAA extensions defined in section 5.4.2.

LMA SHALL process and verify the contents of the PBU received from the target AR/MAG as defined in [81] (and [93] for PMIP6 with IPv4 support). If the PBU parameters are conformant, and if the HAAA has authorized PMIP6 with the appropriate service information indications, the LMA updates the MS's binding cache entry with the new location information storing the new Proxy-CoA address. Upon successfully updating the MS's BCE, the LMA SHALL establish a PMIP6 tunnel towards the new AR/MAG, installs the corresponding forwarding rules and simultaneously tears down the tunnel towards the previous AR/MAG (old Proxy-CoA).

If the AAA indicates in-band protocol security is needed for the ongoing PMIP6 session (i.e., use of AO in PBA/PBU), the LMA SHALL require and derive the necessary security parameters as to protect the PBA before it is sent to the target AR/MAG. If the received PBU did not include the AO protection, though it is required, the LMA SHALL silently discard any such PBU.

The PBU sent in response to the PBU requesting the HO SHALL contain a valid MN ID option, HO indicator option with value set to 3, Access Technology Type set to 5, populated link-local address (value retrieved from the BCE), and the Timestamp option. The remaining PBA fields and mobility options are composed as defined in Table 5-47.

#### 4.8.5.5.5 DHCP Requirements

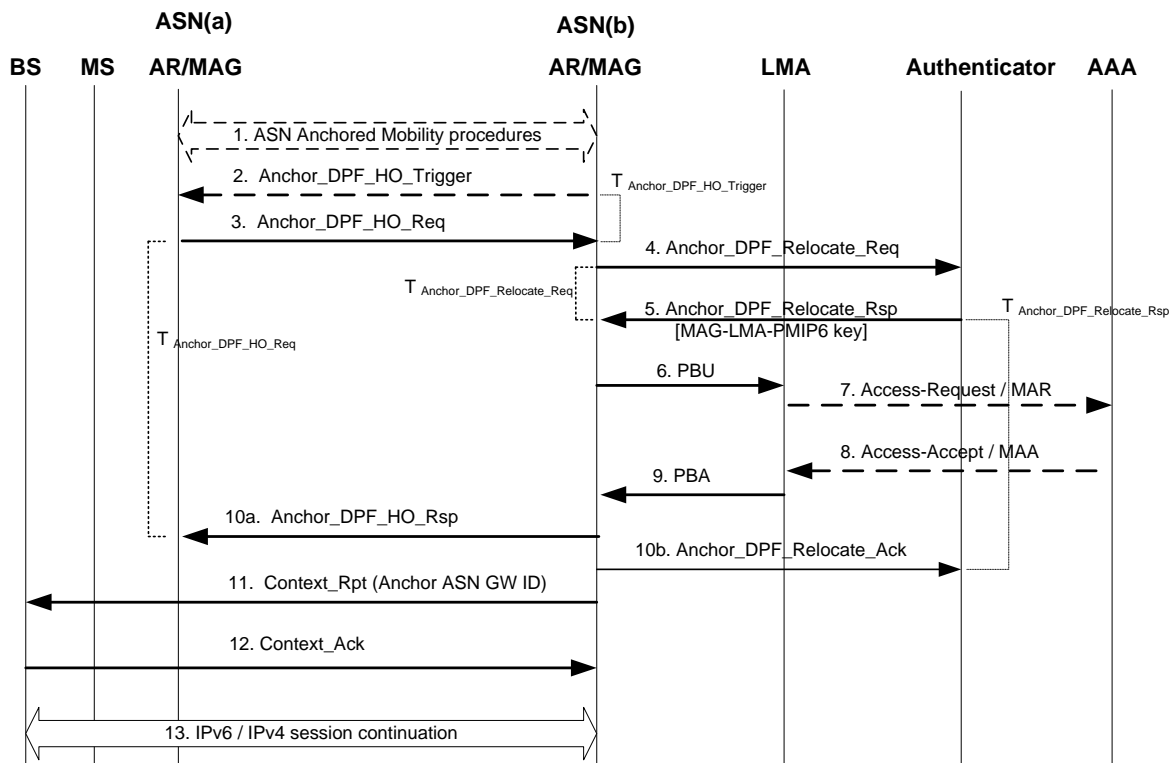
If address configuration mode through DHCP is enabled for ongoing PMIP6 session, the corresponding DHCP Proxy/Relay information MUST be transferred from the anchor ASN(a) to the Target ASN(b) as part of the PMIP6 mobility context.

The Target ASN(b) SHALL process and store the DHCP related parameters obtained in course of the R3 handover within the *Anchor\_DPF\_HO\_Req* message. Presence of the DHCP Proxy Info TLV (with DHCPv6 or DHCPv6 information, depending on the mobility support PMIP6 is providing) indicates the Proxy mode was enabled in the serving ASN(a).

The serving ASN(a) SHALL include the DHCP Relay Info TLV to hint that address configuration mode through DHCP Relay is to be used. The DHCP Relay context, including the Server address(es), and the keying information, SHALL be transferred to the Target ASN(b) as part of the MS mobility context.

#### 4.8.5.5.6 PMIP6 CSN MM Flow(s)

Figure 4-141 presents the PMIP6 CSN Anchored mobility handover procedure for IPv6 and IPv4 MSs.



**Figure 4-141 – PMIP6 CSN Anchored Mobility**

#### STEP 1

MS moves to the new serving gateway ASN(b) as a result of ASN-MM or network optimization procedure.

#### STEP 2

The new serving AR/MAG ASN (b) may trigger the R3 relocation procedure by sending *Anchor\_DPF\_HO trigger* message to the old Anchor DPF ASN(a).

#### STEP 3

The anchor AR/MAG ASN(a) initiates the R3 relocation by sending the *Anchor\_DPF\_HO\_Req* message (starts the *Anchor\_DPF\_HO\_Trigger* timer). In case of a Pull Mode HO, the anchor ASN(a) responds to the trigger message received from the new serving ASN(b) in Step 2.

#### STEP 4

The Target ASN(b) sends *Anchor\_DPF\_Relocate\_Req* to the Anchor Authenticator requesting a DPF relocation. If in-band PMIP6 security was indicated in the PMIP6 context obtained from the anchor ASN(a) in step 3, the target ASN(b) requests the necessary PMIP6 key information from the Authenticator by including the Context Purpose Indicator TLV (with bit #11 set).

#### STEP 5

If the Anchor Authenticator grants the relocation request, the Anchor Authenticator derives and returns the requested MAG-LMA-PMIP6-Key (valid for the specific MAG, LMA and MN triplet only) in the *Anchor\_DPF\_Relocate\_Rsp* message to the serving ASN(b).

# **STEP 6**

The AR/MAG ASN(b) sends a *Proxy Binding Update* message to the LMA. The PBU message is formed as described in section 4.8.5.5.3. If in-band protocol security is enabled, then the PBU includes a valid MAG-LMA derivation in the MN-HA mobility message authentication option [71].

# **STEP 7**

If required, the LMA sends an AAA request to the AAA server to authorize MS's PMIP6 session, and to obtain necessary or new security parameters in case in-band signaling protection is enabled. The AAA request contains the *PMIP6 Service Information TLV*.

# **STEP 8**

If the IP service is permitted, the AAA server responds to the LMA including the PMIP6 session authorization indication(s) in the WiMAX-Capability, and provides additional protocol feature hints in the *PMIP6-Service-Info* attribute.

# **STEP 9**

The LMA updates the BCE for the MS, sends a *Proxy Binding Acknowledgement* message (described in section 4.8.5.5.4) to the AR/MAG in ASN(b) and creates the transport tunnel between itself and the AR/MAG in ASN(b). If in-band signaling protection is enabled, PBA message includes the correct MN-HA mobility message authentication option.

# **STEP 10**

Upon receiving the *Proxy Binding Acknowledgement* message, the AR/MAG in ASN (b) creates the tunnel towards the LMA and sends the *Anchor\_DPF\_HO\_Rsp* to the old anchor AR/MAG ASN(a). Previous anchor AR/MAG ASN(a) stops the timer  $T_{\text{Anchor\_DPF\_HO\_Trigger}}$  and releases the resources related with MS's PMIP6 session. ASN(b) also sends an *Anchor\_DPF\_Relocate\_Ack* updating the Anchor Authenticator regarding the PBU registration status.

# **STEP 11**

ASN(b) sends the *Context\_Rpt* message containing IP address of the new Anchor DPF function to the serving BS.

# **STEP 12**

Upon receipt of the *Context\_Rpt*, the BS updates the location of the Anchor DPF function for the attached MS and confirms the action by sending the *Context\_Ack* message.

# **STEP 13**

The new anchor AR/MAG ASN(b) applies the default-router configuration as specified in [81] (and [93] for IPv4 MS) for all subsequent IP packets exchanged with the MS, to achieve appearance of the same link attachment and thus uninterrupted IP session continuity for the MS.

*Anchor\_DPF\_HO\_Req* message sent from the anchor ASN to the serving ASN for PMIP6 handover is defined as shown below in Table 4-137:

**Table 4-137 – Anchor\_DPF\_HO\_Req Message**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>Authenticator ID	5.3.2.19	M	
>DHCP Relay Info	5.3.2.56	O	Information about the DHCP Relay. Anchor ASN SHALL include this TLV if

IE	Reference	M/O	Notes
			operating in PMIP6 DHCPv4 or DHCPv6 Relay mode.
>>DHCP Server Address	5.3.2.57	O	The IPv4 or IPv6 address of the DHCP Server.
>>DHCP Relay Address	5.3.2.55	O	DHCP Relay IPv4 or IPv6 address for which the key is requested.
>>DHCP Key	5.3.2.51	O	Key used to calculate and authenticate messages between the DHCP relay and DHCP server.
>>DHCP Key ID	5.3.2.52	O	Key ID associated with the key used to compute authentication suboption.
>>DHCP Key Lifetime	5.3.2.53	O	The remaining lifetime in seconds of the DHCP key.
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	The TLV contains one or more packet classification rules.
>>>Classification Rule Index	5.3.2.30	CM	This TLV SHALL be included if Packet Classification Rule / Media Flow Description is included in the transmitted message.
>>>Classification Rule Priority	5.3.2.32	O	The value of the field specifies the priority for the Classification Rule.
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	The values of the field specify the matching parameters for the IP type of service/DSCP byte range and mask.
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...
>>>IP Source Address and Mask	5.3.2.84	O	An IP source address and its corresponding address mask.
>>>IP Destination Address and Mask	5.3.2.82	O	An IP destination addresses and its corresponding address mask.
>>>Protocol Source Port Range	5.3.2.140	O	The value of the field specifies a range of protocol Source port values.
>>>Protocol Destination Port Range	5.3.2.139	O	The value of the field specifies a range of protocol destination port values.
>>>Associated PHSI	5.3.2.15	O	The Associated PHSI value.
>Anchor MM Context	5.3.2.11	M	DHCP Proxy Info, DHCP Server List, MIP4 Info, etc.
>>MS Mobility Mode	5.3.2.104	M	This TLV SHALL be set to indicate PMIP6.
>>DHCP Proxy Info	5.3.2.54	O	Anchor ASN SHALL include this TLV when operating in PMIP6 Proxy DHCP mode.
>>>IP Remained Time	5.3.2.83	O	Remaining lease time for the assigned IPv4 or IPv6 address. This TLV SHALL be included if DHCP Proxy Info is included in the transmitted

IE	Reference	M/O	Notes
			message.
>>> DHCP Proxy Type	5.3.2.418	O	Indicator showing if DHCPv4 or DHCPv6 Proxy function is associated with this request.
>>Idle Mode Info	5.3.2.80	O	
>>PMIP6 Info	5.3.2.412	M	PMIP6 mobility session context
>>>Home Address (HoA)	5.3.2.77	O	IPv4 MN-HoA when PMIP6 mobility is operated for an IPv4 MS
>>> LMA IPv6 Address	5.3.2.413	M	IPv6 address of the associated LMA
>>> LMA IPv4 Address	5.3.2.414	O	If IPv4 transport is used on R3, this TLV contains the IPv4 address of the associated LMA.
>>> Home Network Prefix (HNP)	5.3.2.416	O	PMIP6 Home Network Prefix assigned to the MS
>>> PMIP6 Security Indicator	5.3.2.417	M	Indication for the use of in-band signaling protection
>>> MAG IPv6 Address	5.3.2.415	M	
>PPAQ	5.3.2.131	O	Used during PPA Relocation. This TLV (both expended and the original Quota) SHALL be included if online accounting is activated in the Serving ASN.
>>Quota Identifier	5.3.2.148	CM	This TLV SHALL be included if PPAQ is included in the transmitted message.
>>Volume Quota	5.3.2.167	O	
>>Volume Threshold	5.3.2.168	O	
>>Volume Used	5.3.2.357	O	
>>Duration Quota	5.3.2.275	O	
>>Duration Threshold	5.3.2.276	O	
>> Duration Used	5.3.2.132	O	
>>Resource Quota	5.3.2.277	O	
>>Resource Threshold	5.3.2.278	O	
>>Update Reason	5.3.2.279	O	
>>Service-ID	5.3.2.280	O	
>>Rating-Group-ID	5.3.2.281	O	
>>Termination Action	5.3.2.282	O	
>>Pool-ID	5.3.2.283	O	
>>Pool-Multiplier	5.3.2.284	O	
>>Prepaid Server	5.3.2.285	O	This TLV SHOULD be included if available (provided by HAAA).
>>SFID (one or more)	5.3.2.184	O	SF ID(s) SHALL be included in flow based

IE	Reference	M/O	Notes
			prepaid accounting scenario.
PPAC	5.3.2.65	O	Describes the Prepaid Capabilities of the ASN. This TLV SHALL be included if online accounting is activated in the Serving ASN for the particular MS session. If Target ASN does not support any of the required online accounting capabilities, it SHOULD reject Anchor DPF relocation procedure.
>AvailableInClient	5.3.2.89	CM	This TLV SHALL be included if PPAC is included in the transmitted message.

**Table 4-138 – Anchor\_DPF\_Relocate\_Req from Target ASN to Authenticator ASN**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	O	TLV will be included when the target ASN requests PMIP6 keying information (by setting bit #11 – Security Context delivery)
MS Info	5.3.2.103	M	
> MS Authorization Context	5.3.2.100	M	
>> MS NAI	5.3.2.105	M	
>> PMIP-Authenticated-Network-Identity	5.3.2.41	O	When this TLV is included, its value will be interpreted as the MN ID parameter for PMIP6 at the Authenticator.
>> R3 WiMAX Capability	5.3.2.207	M	
>>> R3 WiMAX-Release	5.3.2.441	M	
>>> R3 Accounting Capabilities	5.3.2.208	M	
>> R3 WiMAX Session ID	5.3.2.214	CM	
>> R3 Packet Flow Descriptor	5.3.2.215	CM	
> Anchor MM Context	5.3.2.11	M	
>>MS Mobility Mode	5.3.2.104	M	Value set to PMIP6
>> PMIP6 Info	5.3.2.412	M	PMIP6 mobility session context
>>> Home Network Prefix (HNP)	5.3.2.416	O	Home Network Prefix assigned to the MS
>>> Home Address (HoA)	5.3.2.77	O	IPv4 MN-HoA when operating PMIP6 mobility for an IPv4 MS
>>> MAG IPv6 Address	5.3.2.415	M	IPv6 address of the target MAG, needed at the Authenticator for key derivation.

**Table 4-139 – Anchor\_DPF\_Relocate\_Rsp from Authenticator ASN to Target ASN**

IE	Description	M/O	Notes
Context Purpose Indicator	5.3.2.36	O	TLV is included when the message delivers PMIP6 security context (bit #11 is set).
MS Info	5.3.2.103	O	
PMIP6 Security Info	5.3.2.419	O	PMIP6 key and associated security parameters
> MAG-LMA-PMIP6 Key	5.3.2.420	O	The requested MS's PMIP6 key specific for the MAG-LMA pair
> MAG-LMA-PMIP6 SPI	5.3.2.421	O	Same value as the SPI of PMIP6-RK
> MAG-LMA-PMIP6 Lifetime	5.3.2.422	O	Time for MAG-LMA-PMIP6 remaining valid
Result Code	5.3.2.154	O	Provide result status for this message. If the result status is any value other than 0, then this TLV SHALL be included

**Table 4-140 – Anchor\_DPF\_Relocate\_Ack from Target ASN to Authenticator ASN**

IE	Description	M/O	Notes
Result Code	5.3.2.154	O	Provide result status for this message. If the result status is any value other than 0, then this TLV SHALL be included

#### 4.8.5.5.7 Handover timers and timer considerations

This section provides the description of the timer used during PMIP6 CSN MM Handover.

- $T_{\text{Anchor\_DPF\_HO\_Trigger}}$ : is started by target ASN(b) upon sending an *Anchor\_DPF\_HO\_Trigger* message. It is stopped upon receiving a corresponding *Anchor\_DPF\_HO\_Req*.
- $T_{\text{Anchor\_DPF\_HO\_Req}}$ : is started when serving ASN(a) sends an *Anchor\_DPF\_HO\_Req* and is stopped upon receiving a corresponding *Anchor\_DPF\_HO\_Rsp*.
- $T_{\text{Anchor\_DPF\_Relocate\_Req}}$ : is started by the target ASN(b) when the *Anchor\_DPF\_Relocate\_Req* is sent on R4. It is stopped upon receiving a corresponding *Anchor\_DPF\_Relocate\_Rsp* from the Anchor Authenticator.
- $T_{\text{Anchor\_DPF\_Relocate\_Rsp}}$ : is started by the Anchor Authenticator when the *Anchor\_DPF\_Relocate\_Rsp* is sent on R4. It is stopped upon receiving a corresponding *Anchor\_DPF\_Relocate\_Ack* from the target ASN(b).

Table 4-141 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-141 – Timer Values for PMIP6 CSN MM Handover Messages over R4/R3**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{\text{Anchor\_DPF\_HO\_Trigger}}$	TBD		TBD



Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
T <sub>Anchor_DPF_HO_Req</sub>	TBD		TBD
T <sub>Anchor_DPF_Relocate_Req</sub>	TBD		TBD
T <sub>Anchor_DPF_Relocate_Rsp</sub>	TBD		TBD

#### 4.8.5.5.8 Handover error conditions and recovery

This section describes error conditions associated with the PMIP6 CSN MM Handover procedure.

##### 4.8.5.5.8.1 Timer Expiry

Table 4-142 shows details on the corresponding actions associated with timer expiry. 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 4-142 Timer Max Retry Conditions.

**Table 4-142 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T <sub>Anchor_DPF_HO_Trigger</sub>	Target AR/MAG	PMIP6 CSN MM handover is aborted and further action of Serving/Target AR/MAG is implementation specific.
T <sub>Anchor_DPF_HO_Req</sub>	Serving AR/MAG	PMIP6 CSN MM handover is aborted and further action of Serving/Target AR/MAG is implementation specific.
T <sub>Anchor_DPF_Relocate_Req</sub>	Target AR/MAG	PMIP6 CSN MM handover is aborted and <i>Anchor_DPF_HO_Rsp</i> is sent to serving ASN(a) with Result Code set to Failure.
T <sub>Anchor_DPF_Relocate_Rsp</sub>	Anchor Authenticator	PMIP6 CSN MM handover is aborted.

##### 4.8.5.5.8.2 Current Proxy CoA mismatches the AR/MAG on Anchor Authenticator

*Anchor\_DPF\_Relocate\_Rsp* with Result Code set to Failure is sent to the sender of *Anchor\_DPF\_Relocate\_Req*, and PMIP6 CSN MM handover is aborted. This message will also trigger *Anchor\_DPF\_HO\_Rsp* with a failure indication.

##### 4.8.5.5.8.3 Proxy Binding Update Failure

Failure of the PBU can be caused due to many reasons, such as authentication or service authorization failure. In such case (Target ASN(b) receiving PBA with a failure code, for example), PMIP6 CSN MM handover is aborted and *Anchor\_DPF\_HO\_Rsp* is sent from Target ASN(b) to the serving ASN(a) with Result Code set to Failure and further action of Serving/Target AR/MAG is implementation specific.

##### 4.8.5.5.8.4 CSN MM HO failure due to a missing feature support

If the Anchor ASN attempts PMIP6 HO to a serving ASN that does not provide PMIP6 mobility support, it SHALL result in a failure of the Anchor DPF relocation request. Presence of PMIP6 Info TLV in *Anchor\_DPF\_HO\_Req* message is an explicit indication to the serving/target ASN that R3 relocation is requested because of the PMIP6

handover. Serving ASN not supporting mobility with PMIP6 SHOULD respond sending the *Anchor\_DPF\_HO\_Rsp* message that includes Result Code TLV set to failure (Error code = 0x02, Failure – Not supported).

#### 4.8.5.6 PMIP6 Session Termination

The PMIP6 session termination may be instigated by following network entities:

- MS MAY initiate this procedure when triggering graceful shutdown procedure or releasing the allocated IP address.
- ASN-GW (AR/MAG and A-DPF) MAY trigger termination based either on internal failure situation, such as loss of radio connectivity, or graceful shutdown trigger.
- HAAA server
- LMA

##### 4.8.5.6.1 AAA/NAS Requirements

The HAAA server in the HCSN MAY initiate request for PMIP6 session termination for a number of configurable or policy reasons. The followings are major reason for such termination:

- Change in service strategy affecting the subscriber mobility privileges.
- Loss of mobile device

In case AAA server originates session termination request, it SHALL send either the RADIUS Disconnect message or Diameter WASR message to the Anchor Authenticator (NAS) triggering common procedure for ASN data path release and MIP De-Registration described in section 4.5.1.2.4.

##### 4.8.5.6.2 AR/MAG Requirements

In the case that the AR/MAG detects a failure situation, it SHOULD initiate the termination of PMIP6 session. An example of such event is a failure where MS re-initialization is needed, hence established data paths and IP transport connections need to be torn down.

If receiving a De-Registration notification, the AR/MAG SHALL initiate PMIP6 session termination by sending the PBU message with the lifetime set to 0 to the designated LMA. Upon obtaining acknowledgement of the successful session termination the AR/MAG removes the specific BCE and releases associated states and resources. Any subsequent session termination event related with the previously released session, if any received (e.g., BRI from the LMA), SHALL be ignored.

If receiving a valid BRI message from a known LMA, the AR MAG SHALL release allocated BCE and resources and acknowledge session termination sending BRA to the revocation originator. Concurrent or subsequent termination triggers for the same session SHALL be ignored.

##### 4.8.5.6.3 LMA Requirements

The LMA MAY decide to trigger termination of an ongoing PMIP6 session in case the it detected expiry of the MS's binding lifetime or another event eligible to trigger forced network exit. In those cases the LMA SHALL trigger PMIP6 session termination for the specific MS's IP session invoking the Binding Revocation procedure with the currently associated MAG. In case of DHCPv4/v6 Relay mode, and upon receiving a DHCPv4/v6 Release message forwarded by the DHCP Relay function, the (non)collocated DHCPv4/v6 server MAY trigger the LMA to terminate the PMIP6 session, remove specific BCE and initiate R3 tunnel tear down by sending the BRI to the associated MAG. The LMA SHOULD also accept PBU message from a trusted MAG with the lifetime set to zero as the session termination trigger, if such message is received.

##### 4.8.5.6.4 DHCP Requirements

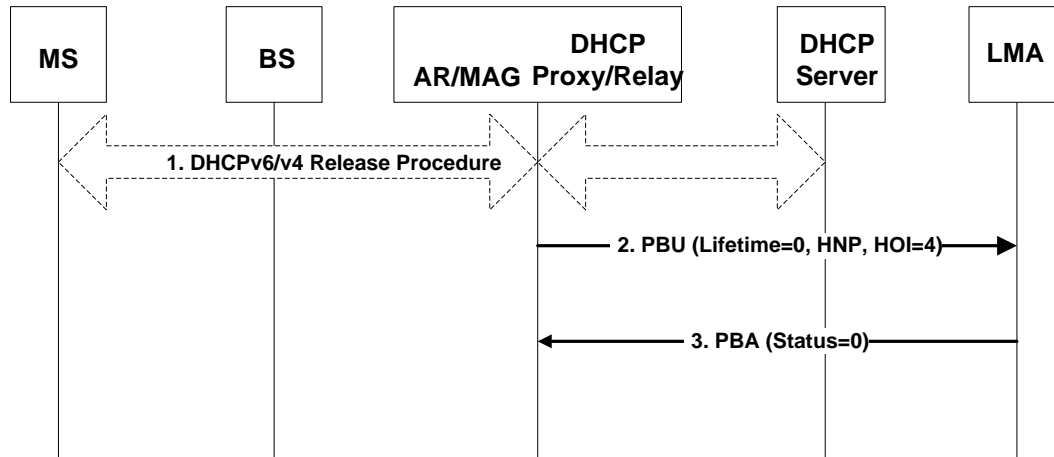
Upon receiving DHCPv4/v6 Release message DHCP Proxy entity notifies AR/MAG function it is collocated with to perform MIP De-Registration for the MS's PMIP6 session. De-Registration procedure SHALL also get triggered in case DHCP lease time for the assigned IPv4 MN-HoA or IPv6 HNP expires. If De-Registration is successfully acknowledged by the LMA, DHCP Proxy entity SHALL release the HoA address or HNP, and associated states and resources.

The DHCPv4/v6 Relay SHALL relay the intercepted DHCP Release message to the designated DHCPv4/v6 Server.

#### 4.8.5.6.5 PMIP6 Session Termination Flows

##### 4.8.5.6.5.1 MS or MAG Session Termination

Figure 4-142 presents PMIP6 session termination procedure initiated by MS or the ASN-GW.



**Figure 4-142 - PMIP6 Session Termination by MS / MAG**

#### STEP 1

In case the ASN-GW (A-DPF) detects a reason for PMIP6 session termination it initiates data path de-registration along the R4/R6 path with the serving BS even prior to step 1. The MS initiates the IP session release by performing DHCPv6 Release Procedure (DHCPv4 Release in case of an IPv4 MS) either self-initiated (MS triggered termination) or in response to the DREG directive received (ASN-GW triggered). For an IPv6 MS that was using stateless address autoconfiguration there will not be a DHCPv6 release procedure. In such a case the MS has no means to inform the network it wants to terminate the IPv6 session, so the MS initiates the network exit procedure by sending *DREG\_REQ* message with De-Registration Request Code=0x00 to the BS.

#### STEP 2

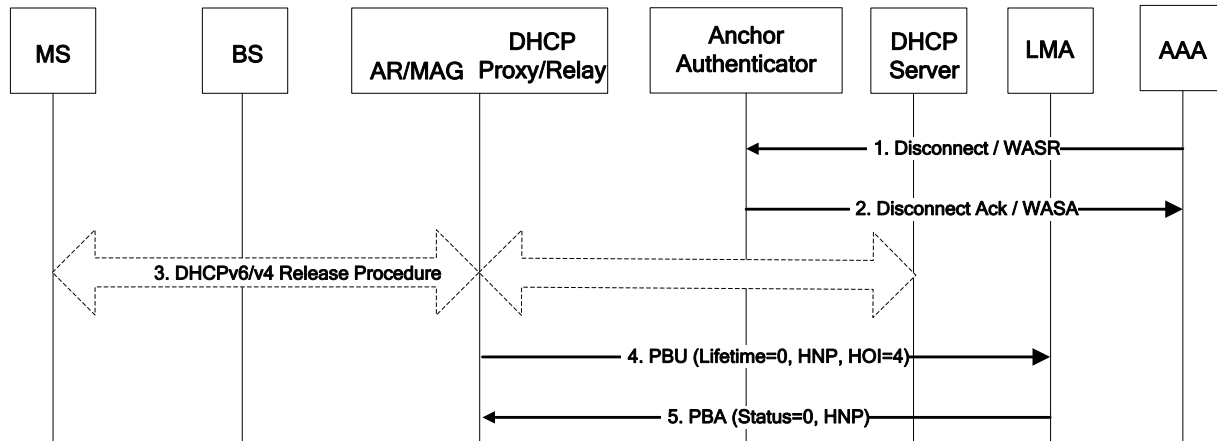
The AR/MAG discovers that the MS has performed L3 release or has detached from the network and sends a PBU to the associated LMA signaling MS detachment and binding de-registration. The PBU is constructed as specified in [81]; it has the Lifetime field value set to zero, must contain the HNP/IPv4-HoA assigned to that MS and must set the Handover Indicator (HOI) option to value 4.

#### STEP 3

The LMA processes the PBU, removes and releases corresponding resources from the binding cache and its routing state and constructs the PBA response for the source MAG/AR. If the de-registration was successful, the PBA Status field is set to value zero, the HNP and HOI values are same as received in the PBU. Succeeding data path deregistration, NetExit and Accounting Stop procedures SHALL take place as specified in section 4.5.2.1.1

#### 4.8.5.6.5.2 AAA Session Termination

Figure 4-143 presents PMIP6 session termination procedure by the AAA.



**Figure 4-143 - PMIP6 Session Termination by AAA**

### STEP 1

The Home AAA server induces PMIP6 session termination issuing the RADIUS Disconnect packets or Diameter WiMAX Abort Session Request (WASR) message to the ASN-GW/ASN hosting the Anchor Authenticator.

### STEP 2

Anchor Authenticator ASN acknowledges the Disconnect message by sending either RADIUS Disconnect-ACK or DIAMETER WiMAX Abort Session Answer (WASA) message to the AAA. In parallel, the Authenticator signals the MS state change to the Anchor DPF ASN-GW/ASN and initiates the R4/R6 data path deregistration following the procedure defined for AAA initiated network exit (section 4.5.2.1.2.1).

### STEP 3

As part of the network-triggered path deregistration, the L3 release and detach procedure takes place in response to the DREG directive. If the MS used DHCP for the HNP/MN-HoA acquisition it performs the DHCPv6/v4 Release Procedure. There may not be a DHCPv6 release procedure when PMIP6 connection setup was achieved through address autoconfiguration.

### STEP 4

The AR/MAG discovers the MS release/detach and instigates PMIP6 binding release with the LMA as part of the MS Network Exit procedure by sending the PBU with the Lifetime field set to value zero (also including corresponding MN-ID, HNP/MN-HoA and HOI=4 information).

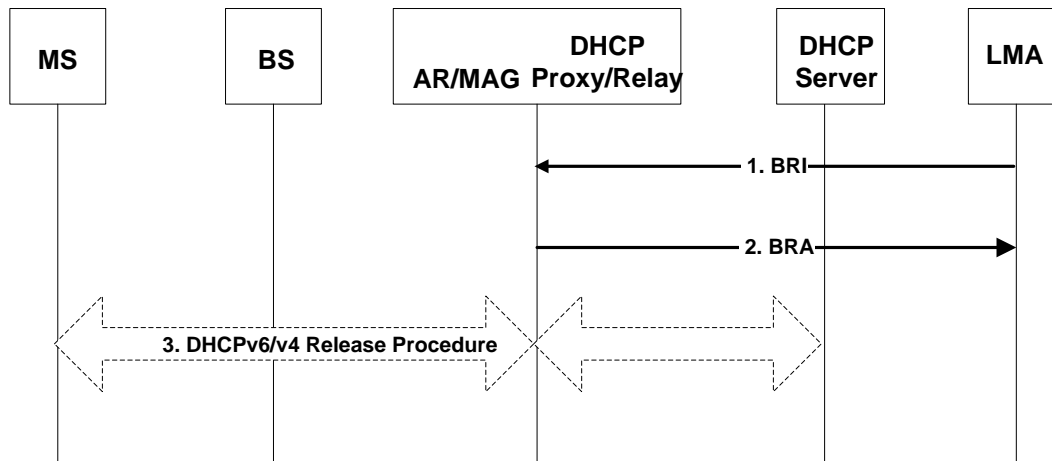
### STEP 5

After successfully processing the De-registration PBU, the LMA releases the BCE and removes the forwarding tunnel(s) for the specific HNP/MN-HoA. Removal of MS's mobility binding is acknowledged with the appropriate PBA sent back to the AR/MAG.

The session termination is completed through R4/R6 data path deregistration and Accounting stop procedures as described in section 4.5.2.1.2.1.

#### 4.8.5.6.5.3 LMA Session Termination

Figure 4-144 presents PMIP6 session termination procedure by LMA.



**Figure 4-144 - PMIP6 Session Termination by LMA**

### STEP 1

If the MS's mobility binding expires or gets terminated, the LMA initiates PMIP6 session release by sending the Binding Revocation Indication (BRI) message to the AR/MAG (Proxy-CoA) for the MS attached to it. The BRI message sets the "A" and "P" bits, and contains the MN ID and the associated HNP/IPv4 MN-HoA, as specified in [95]. If the initial binding registration for the MS was protected using the authentication extension option, the BRI is sent protected in the same way. Additional BRI fields and mobility options are composed as presented in Table 5-48.

### STEP 2

Upon receiving and validating the BRI message, the AR/MAG initiates the data path de-registration along the R4/R6 path towards the serving BS. The MAG then releases the resources and forwarding rules associated with the MS PMIP6 binding, and sends the Binding Revocation Acknowledgement (BRA) to the LMA. The BRA message sets the "P" bit and the corresponding code indicated in the status field (complete message description given in Table 5-48). Only upon receiving the BRA (or retransmit timer expiry), the LMA releases the MS's proxy BCE and the associated forwarding tunnel.

### STEP 3

If the IP address was configured through stateful address configuration the MS performs the DHCPv6 Release Procedure (DHCPv4 Release in case of an IPv4 MS) in response to DREG directive received from the serving BS. The session termination gets completed following data path deregistration, NetExit and Accounting Stop procedures as specified in section 4.5.2.1.2.5

#### 4.8.5.6.6 Handover timers and timer considerations

FFS

#### 4.8.5.6.7 Handover error conditions and recovery

FFS

## 4.9 Radio Resource Management

### 4.9.1 Introduction

RRM is a function performed by the BS in a WiMAX Network, aiming at increasing the radio resource usage efficiency. RRM introduces a concept of Radio Resource Agent (RRA) and Radio Resource Controller (RRC) functional elements and signaling between RRA and RRC and between RRC and RRC (see [stage 2] section 7.7 for more details on RRA and RRC functional entities and their respective responsibilities).

If RRM is supported, then RRC and RRA are located in the BS. See section 4.9.2 and Stage 2 Part 2 section 7.9 for details on RRM reference model.

Moreover, in case of Profile C, RRM may either work without R8 (i.e. based on R6 and R4), or by help of R8 being implemented between the BSs within an ASN (i.e. based on R6, R8 and R4). Both cases are specified here.

Implementation of RRM is optional. This is possible because

- Many RRM tasks, e.g., providing assistance for Service Flow Admission Control, are executed autonomously and locally in each BS without any interaction to other RRM Functional Entities in the ASN.
- Some RRM related signaling is implicitly included in signaling between other ASN functions, as for example:
  - Handover function, e.g., using *HO\_Req* and *HO\_Rsp* to evaluate the spare capacity of candidate Target BSs, and,
  - QoS Function, e.g., SF handling using *RR\_Req* and *RR-Rsp*.

When RRC is not implemented, then also RRA concept and requirements do not apply, i.e., are informative only.

#### 4.9.2 RRM Primitives and their Mapping to Reference Points

These RRM-related primitives MAY be used on references points R6 or R4, or also R8 if available.

The RRC function in each BS controls its local RRA function and communicates with neighboring RRCs in other BSs. RRC-RRC communication may occur directly from BS to BS via the R8 interface, or relayed via the ASN-GW (or ASN-GWs). In the latter, an "RRC Relay" function is present in the ASN-GW (see [stage 2] section 7.7 for more details on RRC Relay). Furthermore, the RRC Relay function facilitates RRM signaling communication between ASN-GWs.

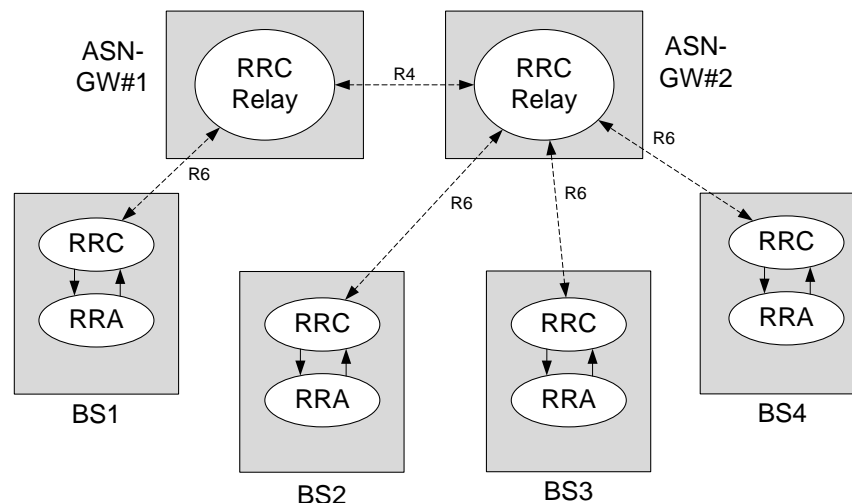
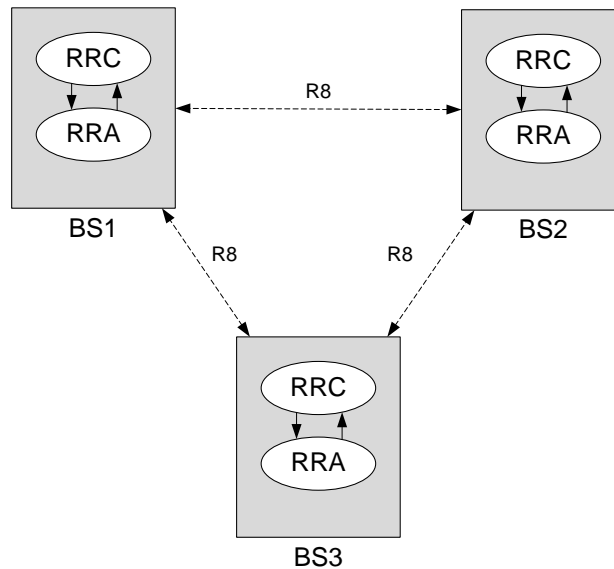


Figure 4-145 –RRC-RRC Communication on R6 and R4



**Figure 4-146 – RRC-RRC Communication on R8 (provided R8 is available)**

The mapping of RRM primitives to R6 and R4, as well as R8 if any, is shown in Table 4-143.

**Table 4-143 – RRM Procedures, Messages, Mapping to Reference Points**

RRM Primitives	Communication Peers	Intra-ASN	Inter-ASN
Per-BS <i>Spare_Capacity_Req</i> and <i>Spare_Capacity_Rpt</i>	RRC – RRC	R4, R6, R8	R4
Per-BS <i>Radio_Config_Update_Req</i> and <i>Radio_Config_Update_Rpt</i> and <i>Radio_Config_Update_Ack</i>	RRC – RRC	R4, R6, R8	R4

Note: For support of Association levels 1 and 2 as specified in [802.16e-2005], section 6.3.22.1.3, additional RRM procedures – or HO preparation procedures - may be required in subsequent releases.

### 4.9.3 RRM Signaling

As can be seen from Figure 4-145 “RRC-RRC Communication on R6 and R4”, RRM messages may occur on R6 and R4. Any RRM messages on R4 are resulting from relaying R6 RRM messages. On R4, RRM messages can only occur in case there is more than one RRC Relay function involved on the path from the originating to the terminating RRC entity.

Since the RRC Relay function is a regular ASN GW Relay function that keeps the relayed message unchanged, the RRM message tables shown below are the same for R6 and R4.

#### 4.9.3.1 Per-BS Spare Capacity Reporting Procedure

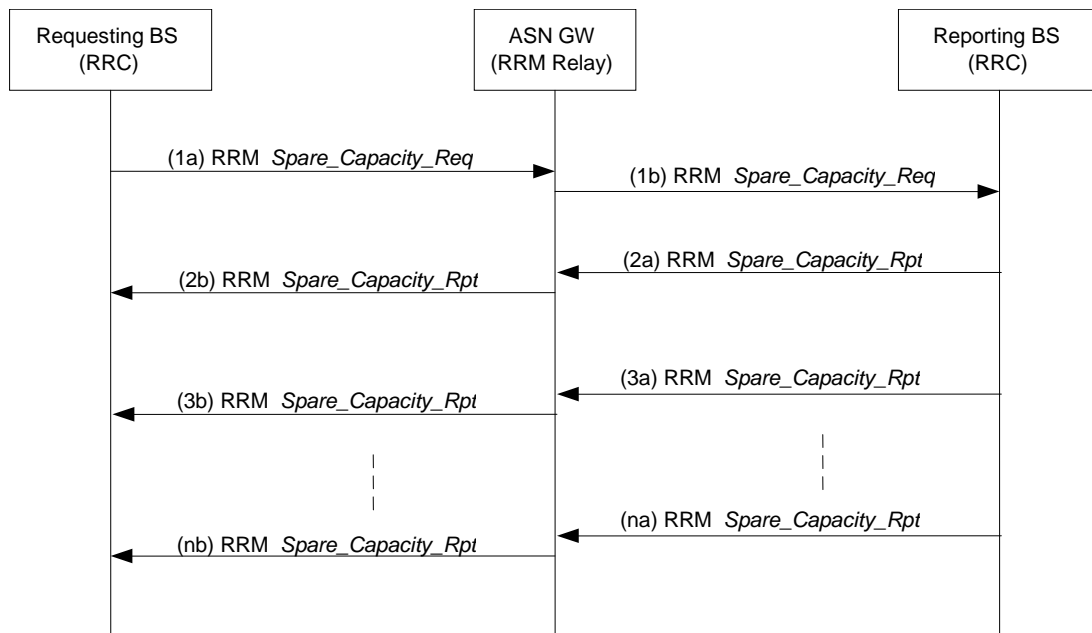
##### 4.9.3.1.1 Per-BS Spare Capacity Reporting Procedure with R6/R4

This procedure MAY be used by a BS (i.e., by the RRC in the BS) to retrieve information about the current load situation of any other BS, in particular of those neighboring Base Stations which MAY become candidate Target BSs (TBSs) for Handover decisions.

Since the BS cannot communicate directly to neighboring BSs, it SHALL send the RRM primitives to a Relay RRC in an ASN GW. The Relay RRC SHALL forward that message to the destination BS, or to another Relay RRC if the destination BS can't be reached directly.

So the same RRM-Spare-Capacity-Req/Report procedure SHALL also be used by the “Relay” RRC in the ASN GW to request Spare Capacity reports from destination Base Stations, in response to Spare\_Capacity\_Req messages received from source BSs.

Figure 4-147 shows the application of this procedure between two BSs (Requesting BS and Reporting BS) with an ASN GW performing the Relay RRC function.



**Figure 4-147 – Per-BS Spare Capacity Reporting Procedure**

#### STEP 1 (1a, 1b)

The "requesting BS" sends an RRM *Spare\_Capacity\_Req* to the ASN GW, requesting it to report about the available radio resources of a certain "Reporting BS"; reporting SHALL be done once, or periodically, or event driven.

The OP ID of this message is 0b001 (“Request/Initialization”).

ASN GW, in its role as RRC Relay, sends the same RRM *Spare\_Capacity\_Req* to the indicated Reporting BS. If that BS can't be reached directly, ASN GW will send the request to other ASN GW working as RRC Relay. In case of two RRC Relays involved, the RRM message will show up on R4 as well.

#### STEP 2 (2a, 2b)

The Reporting BS sends RRM *Spare\_Capacity\_Rpt* to ASN-GW, in direct response to the Request. ASN-GW relays that message to the Requesting BS.

The OP ID of this message is 0b010 (“Response”). This ends the 2-way transaction.

In case of two RRC Relays involved, the RRM message will show up on R4 as well.

#### STEP 3 (3a, 3b, ..., na, nb)

Optionally, the Reporting BS sends RRM *Spare\_Capacity\_Rpt* to ASN-GW, or subsequently in response to predefined events. ASN-GW relays that message to the Requesting BS.



The OP ID of this message is 0b100 (“Indication”). Each of these unsolicited reports is a 1-way transaction of its own.

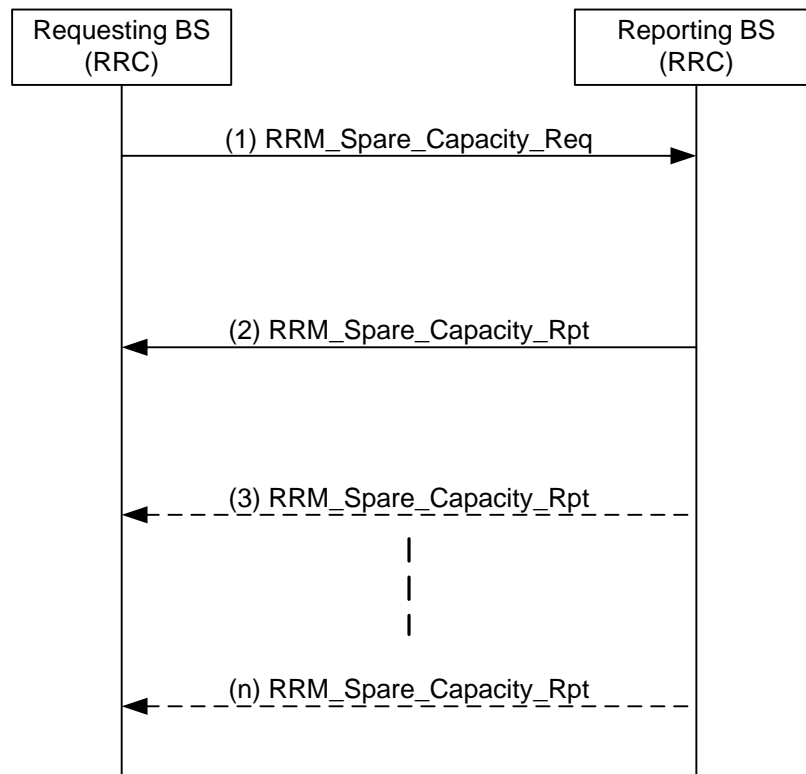
In case of two RRC Relays involved, the RRM message will show up on R4 as well.

In the event of periodic reporting, if the reporting RRC needs to stop sending unsolicited RRM *Spare\_Capacity\_Rpt* to Requesting RRC, it SHALL include Reporting Characteristics TLV with a value of zero (0000) in the final *Spare\_Capacity\_Rpt*.

#### 4.9.3.1.2 Per-BS Spare Capacity Reporting Procedures with R8

In this case, the BS can communicate directly to neighboring BSs via R8.

Figure 4-148 shows the application of this procedure between two BSs (Requesting BS and Reporting BS) directly via R8.



**Figure 4-148 – Per-BS Spare Capacity Reporting Procedure via R8**

#### STEP 1

The “requesting BS” sends an RRM *Spare\_Capacity\_Req* to the Reporting BS, requesting it to report about the available radio resources of the “Reporting BS”; reporting SHALL be done once, or periodically, or event driven.

The OP ID of this message is 0b001 (“Request/Initialization”).

#### STEP 2

The Reporting BS sends RRM *Spare\_Capacity\_Rpt* to the Requesting BS, in direct response to the Request.

The OP ID of this message is 0b010 (“Response”). This ends the 2-way transaction.

### STEP 3 , ..., n

Optionally, the Reporting BS sends RRM Spare\_Capacity\_Rpt to the Requesting BS, periodically, or subsequently in response to predefined events.

The OP ID of this message is 0b100 (“Indication”). Each of these unsolicited reports is a 1-way transaction of its own.

#### 4.9.3.1.3 R4/R6/R8 Messages for Per-BS Capacity Reporting Procedures

This section provides the message definitions for the R4, R6 and R8 messages in support of the Per-BS Spare Capacity Reporting Procedure. See also sections 5.2 and 5.3 for message and TLV definitions.

**Table 4-144 – Spare\_Capacity\_Req**

IE	Reference	M/O	Notes
RRM Spare Capacity Report Type	5.3.2.164	M	
BS Info	5.3.2.26	M	Only a single BS Info TLV can be included
>BS ID	5.3.2.25	M	Identifier of the BS whose Spare Capacity SHALL be reported.
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 <i>Spare_Capacity_Report</i> 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.  Note that a separate message to Stop the RRM Reporting is not specified. The same request message, with RRM Reporting Characteristics value set to zero (0000), SHALL be interpreted as a request to stop the RRM reporting, which SHALL be processed by the receiver immediately and acknowledged with a similar value of zero (0000) in the corresponding RRM Spare capacity report message.
RRM Averaging Time T	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	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.

IE	Reference	M/O	Notes
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.

1

**Table 4-145 – Spare\_Capacity\_Rpt**

IE	Reference	M/O	Notes
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. Error Code 33 = BS out of service.
RRM Spare Capacity Report Type	5.3.2.164	M	
RRM Reporting Characteristics	5.3.2.162	O	Indicates the reason for this report. Value zero (0000) indicates the RRM reporting is being stopped, in response to the request received with same value. The reporting RRM SHALL also include this TLV with value set to zero (0000) in case it decides to stop ongoing periodic reporting.
RRM BS Info	5.3.2.159	M	
>BS ID	5.3.2.25	M	
>Available Radio Resource DL	5.3.2.22	M	This TLV SHALL be omitted if the Failure Indication TLV is included.
>Total Slots DL	5.3.2.191	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>Available Radio Resource UL	5.3.2.23	M	This TLV SHALL be omitted if the Failure Indication TLV is included.
>Total Slots UL	5.3.2.192	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>Radio Resource Fluctuation	5.3.2.142	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>DCD/UCD Configuration Change Count	5.3.2.48	O	Included based on local BS policy. Decision to include this TLV is implementation specific.

#### 4.9.3.2 Per-BS Radio Configuration Update Procedure

##### 4.9.3.2.1 Per-BS Radio Configuration Update Procedure with R6/R4

This procedure MAY be used by a BS to report some critical radio resource configuration update to the serving BS(RRC), such as DCD, UCD burst profile changes.

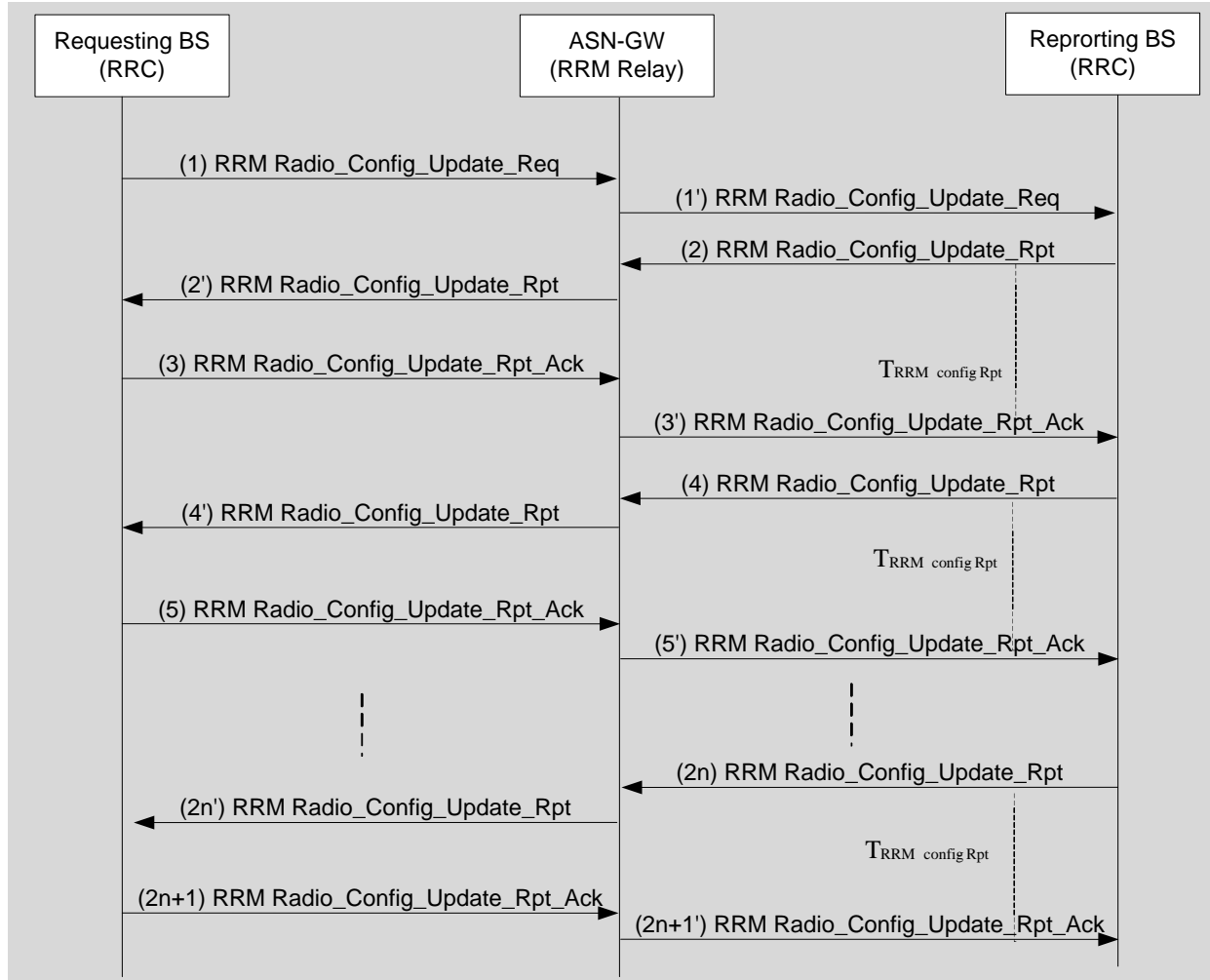


Figure 4-149 – Per-BS Radio Configuration Reporting Procedure

##### STEP 1 , 1'

The “requesting BS” sends an *Radio configuration update-Request* via R6 to the ASN GW, requesting it to report about the radio configuration parameters of one or more “Reporting BSs”; reporting SHALL be done once, or periodically, or event driven to indicate the Radio Configuration parameters whenever these change.

The OP ID of this message is 0b001 (“Request/Initialization”). This is the start of a 3-way transaction.

ASN GW, in its role as RRC Relay, sends the same *Radio configuration update-Request* to the indicated reporting BSs. If a BS can't be reached directly, ASN GW will send the request to other ASN GW working as RRC Relay. In case of two RRC Relays involved, the RRM message will show up on R4 as well.

**STEP 2 , 2'**

The indicated reporting BS sends *Radio Configuration update-Report* to ASN-GW, in direct response to the Request. In addition it sets timer TRRM-config-Rpt, to wait for the *Radio\_Config\_Update\_Ack*. ASN-GW relays the Radio Configuration update-Report message to the Requesting BS.

The OP ID of this message is 0b010 (“Response”).

In case of two RRC Relays involved, the RRM message will show up on R4 as well.

**STEP 3 , 3'**

The Requesting BS acknowledges receipt of *Radio\_Config\_Update\_Rpt* by sending *Radio\_Config\_Update\_Ack* via R6 to ASN GW. ASN GW relays that message to the Reporting BS. Once the Reporting BS receives this Ack message, it stops timer TRRM-config-Rpt.

The OP ID of this message is 0b011 (“Ack”). This ends the 3-way transaction.

In case of two RRC Relays involved, the RRM message will show up on R4 as well.

**STEP 4 , 4'**

In case of periodic or event-driven reporting, the reporting BS sends an unsolicited *Radio Configuration update-Report* to ASN-GW, as requested by the “RRM Reporting Characteristics”, and starts timer TRRM-config-Rpt, to wait for the *Radio\_Config\_Update\_Ack*. ASN-GW relays the *Radio Configuration update-Report* message to the Requesting BS.

The OP ID of this message is 0b100 (“Indication”). It starts a 2-way transaction (Indication – Ack).

In case of two RRC Relays involved, the RRM message will show up on R4 as well.

**STEP 5 , 5'**

The Requesting BS acknowledges receipt of *Radio\_Config\_Update\_Rpt* by sending *Radio\_Config\_Update\_Ack* via R6 to the ASN GW which in turn relays that message to the Reporting BS. Once the Reporting BS receives this Ack message, it stops timer TRRM-config-Rpt.

The OP ID of this message is 0b011 (“Ack”). This ends the 2-way transaction.

In case of two RRC Relays involved, the RRM message will show up on R4 as well.

STEP (2n, 2n';  $n \geq 3$ )

Steps (2n and 2n';  $n \geq 3$ ) are the same as Step 4.

STEP (2n+1, 2n+1';  $n \geq 3$ )

Steps (2n+1 and 2n+1';  $n \geq 3$ ) are the same as Step 5. The 2-way transaction for report and ack may occur repeatedly until the Requesting BS sends another *Radio\_Config\_Update\_Req* for modifying or ending the reporting procedure.

In the event of periodic reporting, if the reporting RRC needs to stop sending unsolicited RRM *Radio\_Config\_Update\_Rpt* to Requesting RRC, it SHALL include Reporting Characteristics TLV with a value of zero (0000) in the final *Radio\_Config\_Update\_Rpt*.

#### 1 4.9.3.2.2 Per-BS Radio Configuration Update Procedure with R8

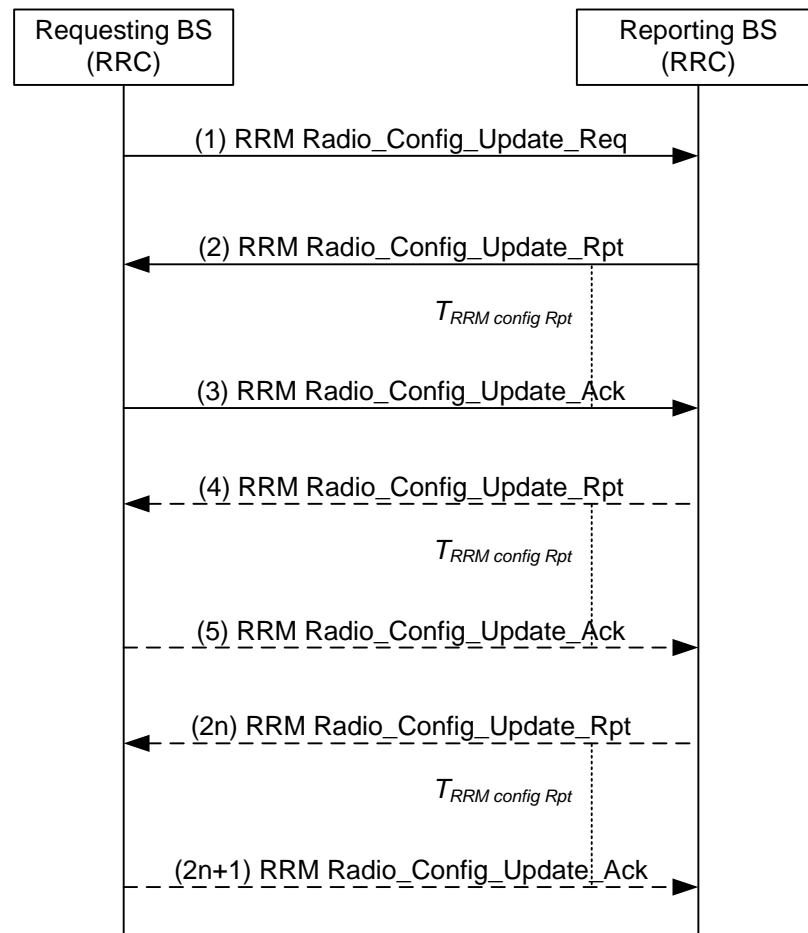


Figure 4-150 – Per-BS Radio Configuration Update Reporting Procedure via R8

#### 4 STEP 1

The “requesting BS” sends a “Radio configuration update-Request” via R8 to each “reporting BS”, requesting it to report about the radio configuration parameters of the “Reporting BSs”; reporting SHALL be done once, or periodically, or event driven, to indicate the Radio Configuration parameters whenever these change.

The OP ID of this message is 0b001 (“Request/Initialization”). This is the start of a 3-way transaction.

#### 9 STEP 2

The reporting BS sends “Radio Configuration update-Report” to the Requesting BS, in direct response to the Request. In addition it sets timer  $T_{RRM\text{-}config\text{-}Rpt}$  to wait for the Radio\_Config\_Update\_Ack.

The OP ID of this message is 0b010 (“Response”).

#### 13 STEP 3

The Requesting BS acknowledges receipt of Radio\_Config\_Update\_Rpt by sending Radio\_Config\_Update\_Ack via R8 to the Reporting BS. Once the Reporting BS receives this Ack message, it stops timer  $T_{RRM\text{-}config\text{-}Rpt}$ .

The OP ID of this message is 0b011 (“Ack”). This ends the 3-way transaction.

#### STEP 4

In case of periodic or event-driven reporting, the reporting BS sends an unsolicited “Radio Configuration update-Report” to the Requesting BS, as requested by the “RRM Reporting Characteristics”, and starts timer  $T_{RRM-config-Rpt}$ , to wait for the Radio\_Config\_Update\_Ack.

The OP ID of this message is 0b100 (“Indication”). It starts a 2-way transaction (Indication – Ack).

#### STEP 5

The Requesting BS acknowledges receipt of Radio\_Config\_Update\_Rpt by sending Radio\_Config\_Update\_Ack via R8 to the Reporting BS. Once the Reporting BS receives this Ack message, it stops timer  $T_{RRM-config-Rpt}$ .

The OP ID of this message is 0b011 (“Ack”). This ends the 2-way transaction.

#### STEP (2n; $n \geq 3$ )

Steps (2n;  $n \geq 3$ ) are the same as Step 4.

#### STEP (2n+1; $n \geq 3$ )

Steps (2n+1;  $n \geq 3$ ) are the same as Step 5. The 2-way transaction for report and ack may occur repeatedly until the Requesting BS sends another Radio\_Config\_Update\_Req for modifying or ending the reporting procedure.

#### 4.9.3.2.3 R4/R6/R8 Messages for Per-BS Radio Configuration Update Procedure

This section provides the message definitions for the R4, R6 and R8 messages in support of the Per-BS Radio Configuration Update Procedure. See also section 5 for message and TLV definitions.

**Table 4-146 – Radio\_Config\_Update\_Req**

IE	Reference	M/O	Notes
BS Info	5.3.2.26	M	Only a single BS Info TLV can be included.
>BS ID	5.3.2.25	M	Identifier of the BSs whose configuration parameters SHALL be reported.
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#3 (whenever DCD/UCD Configuration changes) are applicable, the other bits SHALL be reset. If <i>Radio_Config_Update_Rpt</i> 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 <i>Radio_Config_Update_Rpt</i> SHALL be sent only once. – This TLV is included based on local RRC policy. Decision to include this TLV is implementation specific.  Note that a separate message to Stop the RRM Reporting is not specified. The same request message, with RRM Reporting Characteristics value set to zero (0000), SHALL be interpreted as a request to stop the RRM reporting, which SHALL be processed by the receiver immediately and acknowledged with a similar value of zero (0000) in the corresponding RRM Spare capacity

IE	Reference	M/O	Notes
			report message. The reporting RRM SHALL also include this TLV with value set to zero (0000) in case it decides to stop ongoing periodic reporting.
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

2

**Table 4-147 – Radio\_Config\_Update\_Rpt**

IE	Reference	M/O	Notes
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.
RRM Reporting Characteristics	5.3.2.162	O	Indicates the reason for this report. If the <i>Radio_Config_Update_Req</i> includes multiple events in the reporting characteristics, then the <i>Radio_Config_Update_Rpt</i> can include this attribute to indicate which event triggered the report by setting the corresponding bit position in the attribute. In this message, only Bit#0 (periodic reporting) and Bit#3 (whenever DCD/UCD Configuration changes) are applicable, the other bits SHALL be reset.  Value zero (0000) indicates the RRM reporting is being stopped, in response to the request received with same value.
RRM BS Info	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	5.3.2.25	M	
>DCD/UCD Configuration Change Count	5.3.2.48	O	Included based on local BS policy. Decision to include this TLV is implementation specific.
>Full DCD Setting	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



IE	Reference	M/O	Notes
			and CRC) that the BS will send out in R1 with the new DCD change count.
>Full UCD Setting	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.
> Preamble Index/Sub-channel Index	5.3.2.137	O	Included based on local BS policy. Decision to include this TLV is implementation specific. TC SHALL be set to 1.
>HO Process Optimization	5.3.2.78	O	Included based on local BS policy. Decision to include this TLV is implementation specific. TC SHALL be set to 1.
>Mobility Features Supported	5.3.2.304	O	Included based on local BS policy. Decision to include this TLV is implementation specific. TC SHALL be set to 1.
>PHY Mode ID	5.3.2.410	O	Included based on local BS policy. Decision to include this TLV is implementation specific. TC SHALL be set to 1.
>Scheduling Service Supported	5.3.2.411	O	Included based on local BS policy. Decision to include this TLV is implementation specific. TC SHALL be set to 1.

**Table 4-148 – Radio\_Config\_Update\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
RRM BS Info	5.3.2.159	M	
>BS ID	5.3.2.25	M	A copy of the BS ID which was included in the <i>Radio_Config_Update_Rpt</i> message.

#### 4.9.3.2.4 Radio Configuration Update Procedure Timers and Timing Considerations

This section identifies timer entities defined for the RRM Radio Configuration Update Procedure. The RRM procedure shown in Figure 4-149 employs one timer that is defined as follows:

- RRM configuration report timer ( $T_{RRM-config-Rpt}$ ) – This timer is maintained by an RRC entity in an ASN to monitor the configuration update report.  $T_{RRM-config-Rpt}$  is started upon sending the R4 message *Radio\_Config\_Update\_Rpt*, and it stopped when receiving the *Radio\_Config\_Update\_Ack* message via R4.

**Table 4-149 – RRM configuration report timer.**

Timer	Entity	Reset(s)	Cause(s)	Action(s)
$T_{RRM}$	ASN	Receipt of	Message gets lost due to	When the timer expires, resend

config- Rpt	(RRC)	Radio_Config_Update_Ack	congestion in the backhaul ASN overloaded, unable to process the Radio_Config_Update_Rpt message	the Radio_Config_Update_Rpt, provided the number of retries does not exceed the Radio_Config_Update_Rpt_Retry limit. In case the number of retries would exceed the limit, stop sending the Radio_Config_Update_Rpt and perform error handling based on local policy.
----------------	-------	-------------------------	--	--

Table 4-150 shows the default value of timers and also indicates the range of the recommended timer values.

**Table 4-150 – RRM-config-Rpt Timer Values**

Timer	Default Value (ms)	Criteria	Maximum Timer Value (ms)
RRM-config-Rpt ( $T_{RRM-config\_Rpt}$ )	TBD	TBD	TBD

## 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

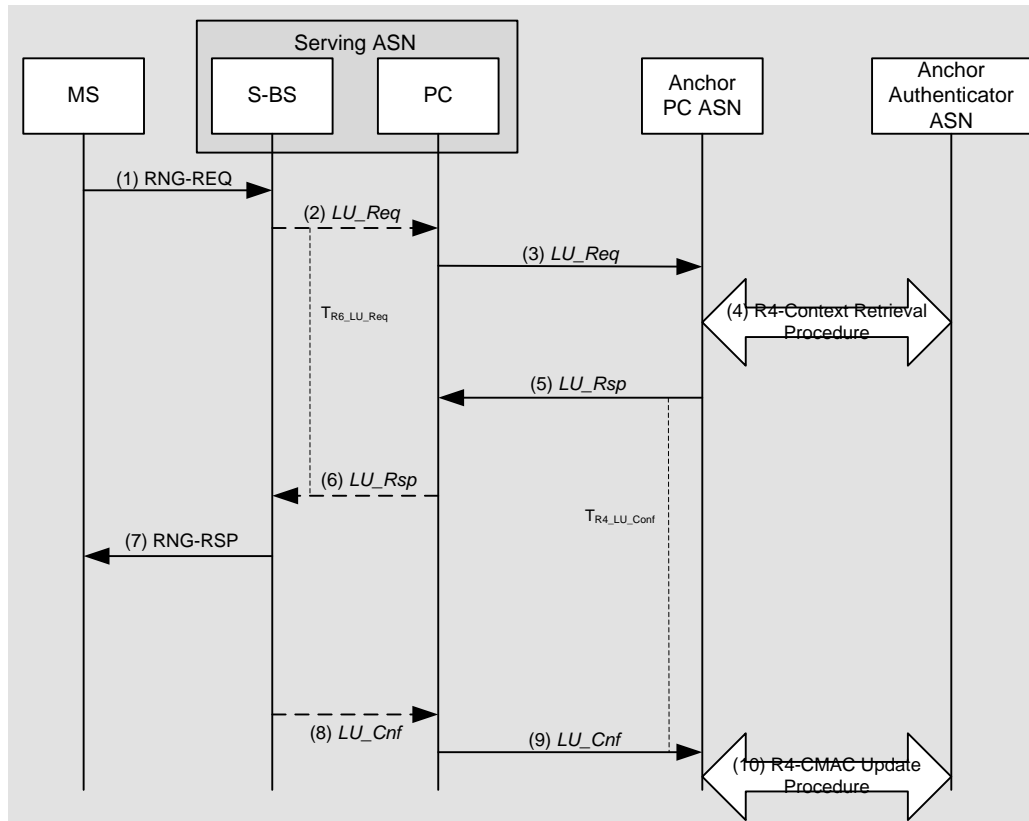
In this section we describe the details of the call flows and the associated messages. For detailed message and TLV formats refer to sections 5.2 and 5.3.

### 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 valid security context which means that BS is not able to receive a valid AK (e.g., MS crossed Mobility Domain boundaries or PMK has expired) or when the BS otherwise elects to direct the MS to proceed with network re-entry. Un-Secure Location Update results in MS network re-entry from Idle Mode. It is performed in the same way as a regular MS network entry process. Anchor PC relocation may occur during Location Update procedure. Anchor PC relocation during location update is an optional procedure. For Location Update with Power Down, refer to section 4.5.2.2.1.

#### 4.10.2.1 Successful Secure Location Update - No Paging Controller Relocation

Figure 4-151 describes a MS initiated successful location update procedure with no Paging Controller relocation.



**Figure 4-151 – Secure Location Update with no Paging Controller Relocation**

### STEP 1

The MS initiates a secure Location Update procedure when the conditions specified in the IEEE Std 802.16e specification are met. The MS sends a RNG-REQ message, which includes the Ranging Purpose Indication TLV set to indicate Idle Mode Location Update, the PC ID TLV which points to the Anchor PC ASN acting as the Anchor PC function for the MS, and the HMAC/CMAC tuple.

### STEP 2

The serving BS sends an R6 *LU\_Req* message to the serving ASN-GW and starts timer  $T_{R6\_LU\_Req}$ . The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the serving BS proposes an update to these parameters.

### STEP 3

The Serving ASN (associated with the serving BS and local PC) sends an R4 *LU\_Req* message to the Anchor PC ASN. The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the Serving ASN proposes an update to these parameters. Note that this message may be relayed by several intermittent ASNs before reaching the Anchor PC ASN.

If the MS mobility access classifier is fixed or nomadic, the Anchor PC checks whether the Serving BS ID belongs to the MS Reattachment Zone. Only if the Serving BS ID belongs to the MS Reattachment Zone, the Anchor PC proceeds with step 4, otherwise it proceeds with step 5 to direct the MS to do initial network entry.

### STEP 4

Anchor PC ASN SHOULD retain context information for the MS including its Authenticator ID, and initiate a Context Request procedure with the Anchor Authenticator ASN. Refer to section 4.12 for the call flow. If the

1 Anchor Authenticator ASN has valid key material for the MS, it returns AK context for the MS to the Anchor PC  
2 ASN.

3 **STEP 5**

4 Upon successful retrieval of the AK context, the Anchor PC ASN sends an R4 *LU\_Rsp* message back to the Serving  
5 ASN and starts timer  $T_{R4\_LU\_Conf}$ . The message includes the MSID, BSID, Authenticator ID, assigned PGID, Paging  
6 Offset, Paging Cycle, Anchor PC ID TLVs, and AK Context.

7 **STEP 6**

8 Upon receipt of the R4 *LU\_Rsp* message, the Serving ASN-GW sends an R6 *LU\_Rsp* message to the S-BS. Upon  
9 receipt the R6 *LU\_Rsp* message, S-BS stops timer  $T_{R6\_LU\_Req}$ . The message includes the, AK Context TLVs, as well  
10 as the assigned Paging Information TLV if they were included in the corresponding R4 message.

11 **STEP 7**

12 Based on the AK and AK context received from the Anchor PC, the Serving BS (associated with Local PC/Relay  
13 PC) successfully authenticates the RNG\_REQ message received from the MS and sends a RNG\_RSP message with  
14 HMAC/CMAC, Successful *LU\_Rsp* indication and New Anchor PC ID as specified in the IEEE Std 802.16  
15 specification, to the MS.

16 **STEP 8**

17 The Serving BS sends an R6 *LU\_Cnf* message to the serving ASN-GW. It includes the CMAC\_Key\_Count in the  
18 R6 *LU\_Cnf*.

19 **STEP 9**

20 The Serving ASN sends an R4 *LU\_Cnf* message to the Anchor PC ASN. Upon receipt of the message, The Anchor  
21 PC ASN updates the LR with MS Idle Mode information and stops timer  $T_{R4\_LU\_Conf}$ .

22 **STEP 10**

23 This step is optional. If Anchor PC ASN receives CMAC Key Count TLV update in *LU\_Cnf* message, it should  
24 perform an R4 CMAC Key Count Update procedure with the Authenticator ASN to update it with the latest CMAC  
25 Key Count. Refer to section 4.13 for the call flow.

#### 4.10.2.2 Successful Secure Location Update with PC Relocation

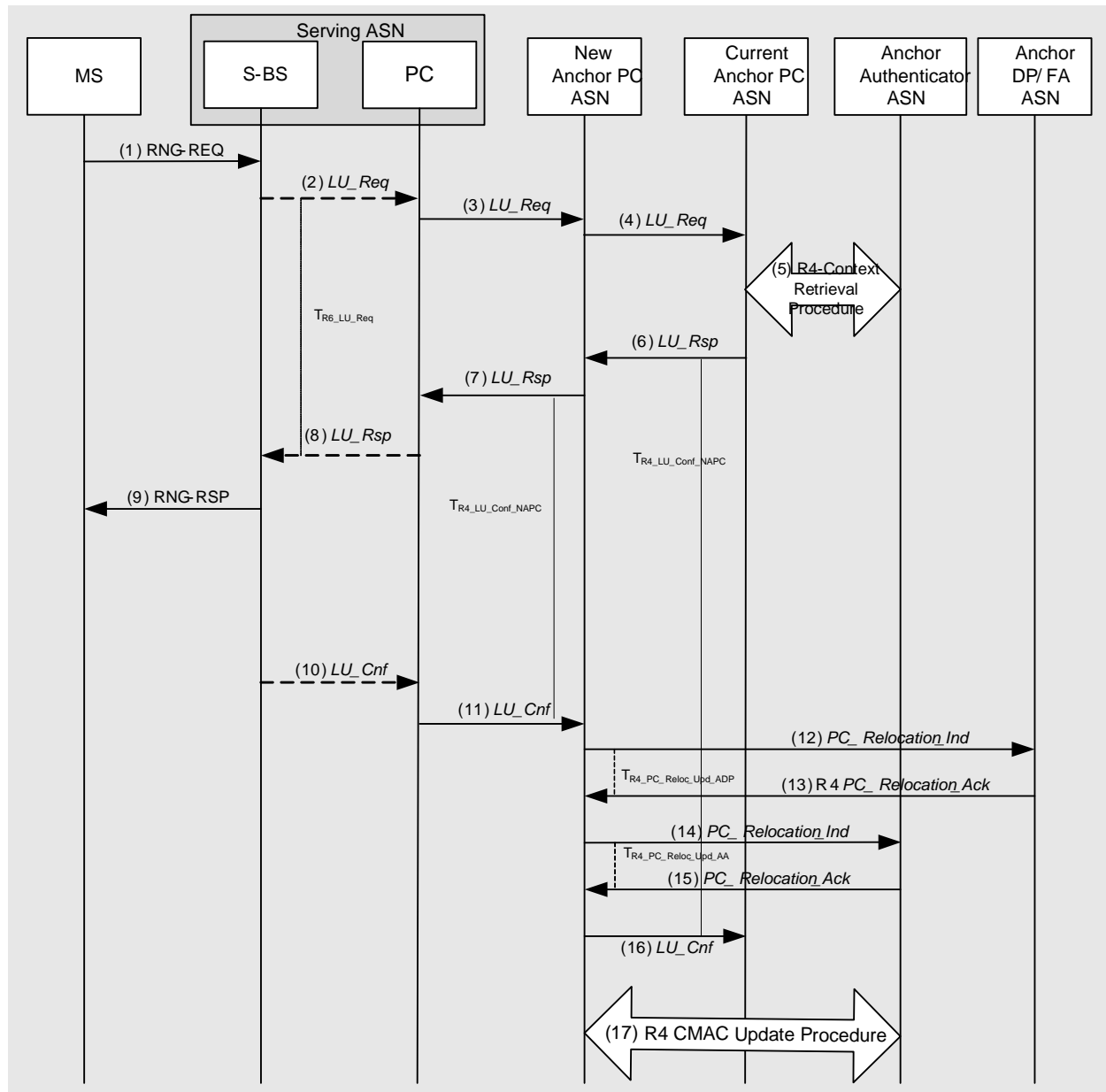


Figure 4-152 – Secure Location Update with Paging Controller Relocation

##### STEP 1

The MS initiates a secure Location Update procedure when the conditions specified in the IEEE Std 802.16e specification are met. The MS sends a RNG-REQ message, which includes the Ranging Purpose Indication TLV set to indicate Idle Mode Location Update, the PC ID TLV which points to the Anchor PC ASN acting as the Anchor PC function for the MS, and the HMAC/CMAC tuple.

**STEP 2**

The serving BS sends an R6 *LU\_Req* message to the serving ASN-GW and starts timer  $T_{R6\_LU\_Req}$ . The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the serving BS proposes an update to these parameters.

**STEP 3**

The Serving ASN (associated with the serving BS and local PC) sends an R4 *LU\_Req* message to the Anchor PC ASN. The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the Serving ASN proposes an update to these parameters. Note that this message may be relayed by several intermittent ASNs before reaching the Current Anchor PC ASN. The Serving ASN or any intermittent ASN along the path may request PC relocation.

**STEP 4**

Upon receipt of the R4 *LU\_Req* message, a relay PC ASN adds the Anchor PC Relocation Destination TLV to initiate PC relocation to it as part of the location update procedure, and forwards the message on to the Anchor PC ASN.

If the MS mobility access classifier is fixed or nomadic, the Anchor PC checks whether the Serving BS ID belongs to the MS Reattachment Zone. Only if the Serving BS ID belongs to the MS Reattachment Zone, the Anchor PC proceeds with step 5, otherwise it proceeds with step 6 to direct the MS to do initial network entry.

**STEP 5**

Refer to section 4.12 for the call flow. If the Current Anchor PC ASN retains context information for the MS including its Authenticator ID, the Current Anchor PC ASN initiates a Context Request procedure with the Anchor Authenticator ASN. If the Anchor Authenticator ASN has valid key material for the MS, it returns AK context for the MS to the Anchor PC ASN.

**STEP 6**

The Current Anchor PC ASN sends an R4 *LU\_Rsp* message back to the New Anchor PC ASN and starts timer  $T_{R4\_LU\_Conf}$ . The message includes the MSID, BSID, Authenticator ID, assigned PGID, Paging Offset, Paging Cycle, Anchor PC ID TLVs, and AK Context. The Anchor PC Relocation Request Response TLV is set to 'Accept' to indicate that the Current Anchor PC ASN accepted the *PC\_Relocation\_Req* and the Anchor PC ID TLV is set to the identifier of New Anchor PC ASN ID which was received in the Anchor PC Relocation Destination TLV in the R4 *LU\_Req* message. The R4 *LU\_Rsp* message also includes MS Info TLV containing MS context for transfer to the New Anchor PC ASN.

If the New Anchor PC ASN doesn't request PC Relocation, the CurrentAnchor PC MAY still request to perform such procedure by including also the PC Relocation Indication TLV. If the New Anchor PC doesn't accept the relocation it will report Failure in step 16.

**STEP 7**

Upon receipt of the R4 *LU\_Rsp* message from Current Anchor PC ASN, New Anchor PC ASN stores the MS context received from Current Anchor PC ASN, updates the Paging Information (Paging Group ID, Paging Cycle, Paging Offset), forwards the R4 *LU\_Rsp* message on to the Serving ASN, and starts timer  $T_{R4\_LU\_Conf\_NAPC}$ .

**STEP 8**

Upon receipt of the R4 *LU\_Rsp* message, the Serving ASN-GW sends an R6 *LU\_Rsp* message to the S-BS. The message includes the MS Info, AK Context, Anchor PC ID, and Old Anchor PC ID TLV. The message may include the Paging Information TLV if they were included in the corresponding R4 message.

**STEP 9**

Based on the AK and AK context received from the Current Anchor PC, the Serving BS (associated with Local PC/Relay PC) successfully authenticates the RNG\_REQ message received from the MS and sends a RNG\_RSP

message with HMAC/CMAC and Successful Location Update Response indication, as specified in the IEEE Std 802.16 specification, to the MS.

#### STEP 10

The Serving BS sends an R6 *LU\_Cnf* message to the serving ASN-GW. It includes the CMAC\_Key\_Count in the R6 *LU\_Cnf*.

#### STEP 11

The Serving ASN sends an R4 *LU\_Cnf* message to New Anchor PC ASN (as indicated by the Anchor PC ID received from the BS). 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  $T_{R4\_LU\_Conf\_NAPC}$ .

#### STEP 12

Upon receipt of the *LU\_Cnf* message, the ‘new’ Anchor PC ASN sends an R4 *PC\_Relocation\_Ind* to the Anchor DP/FA ASN, and starts timer  $T_{R4\_PC\_Reloc\_Upd\_ADP}$ .

#### STEP 13

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 New Anchor PC 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 14

At the same time of sending *PC\_Relocation\_Ind* to Anchor DP/FA, the New Anchor PC sends an R4 PC Relocation Indication to Anchor Authenticator ASN to inform the change of the Anchor PC, and starts timer  $T_{R4\_PC\_Reloc\_Upd\_AA}$ .

#### STEP 15

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 New Anchor PC ASN stops timer  $T_{R4\_PC\_Reloc\_Upd\_AA}$ . 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 16

The New Anchor PC ASN sends an R4 *LU\_Cnf* message with a successful LU indication to the Current Anchor PC ASN. The ‘old’ Current Anchor PC ASN stops timer  $T_{R4\_LU\_Conf}$  and clears its LR context for the MS.

#### STEP 17

This step is optional. If Anchor PC ASN receives CMAC Key Count TLV update in *LU\_Cnf* message, it should perform an R4 CMAC Key Count Update procedure with the Authenticator ASN to update it with the latest CMAC Key Count. Refer to section 4.13 for the call flow.

#### 4.10.2.3 Location Update Timers and Considerations

The following timers are used to support Idle Mode Location Updates:

- $T_{R4\_LU\_Conf}$ : This timer is started upon transmission of an R4 *LU\_Rsp* message by a current Anchor AN. This timer is stopped upon reception of an R4 *LU\_Cnf* message.

- $T_{R4\_LU\_Cnf\_NAPC}$ : This timer is started by a new Anchor PC ASN upon transmission of an R4 *LU\_Rsp* message by a source ASN to a target ASN. This timer is stopped upon reception of an R4 *LU\_Cnf* from the target ASN.
- $T_{R4\_PC\_Reloc\_Upd\_ADP}$ : This timer is started by a ‘new’ Anchor PC ASN upon transmission of an R4 *PC\_Relocation\_Ind* message to an Anchor DP/FA ASN. This timer is stopped upon reception of an R4 *PC\_Relocation\_Ack* message from an Anchor DP/FA ASN.
- $T_{R4\_PC\_Reloc\_Upd\_AA}$ : This timer is started by a ‘new’ Anchor PC ASN upon transmission of an R4 *PC\_Relocation\_Ind* message to an Anchor Authenticator ASN. This timer is stopped upon reception of an R4 *PC\_Relocation\_Ack* message from an Anchor Authenticator ASN.
- $T_{R6\_LU\_Req}$ : This timer is started by a Serving BS upon transmission of an R6 *LU\_Req* message from a Serving BS to a Serving ASN-GW. This timer is stopped upon reception of an R6 *LU\_Rsp* message from the Serving ASN-GW.

Table 4-151 describes the default value and recommended range and duration for these timers.

**Table 4-151 – Location Update Timer Values**

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R4\_LU\_Conf}$	TBD		TBD
$T_{R4\_LU\_Cnf\_NAPC}$	TBD		TBD
$T_{R4\_PC\_Reloc\_Upd\_ADP}$	TBD		TBD
$T_{R4\_PC\_Reloc\_Upd\_AA}$	TBD		TBD
$T_{R6\_LU\_Req}$	TBD		TBD

#### 4.10.2.4 Location Update Error Procedures

##### 4.10.2.4.1 Timer MAX Retries

Table 4-152 describes timer expiry causes, reset triggers and corresponding actions. Upon timer expiry, if the maximum number of retries has not exceeded, the timer is restarted. Otherwise, the corresponding action(s) should be performed as indicated in Table 4-152.

**Table 4-152 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
$T_{R4\_LU\_Conf}$	Anchor PC ASN/Relay ASN	Anchor PC ASN refrains from updating LR with MS Idle Mode info.
$T_{R4\_LU\_Cnf\_NAPC}$	New Anchor PC ASN	Notifying Anchor PC ASN of failure.
$T_{R4\_PC\_Reloc\_Upd\_ADP}$	New Anchor PC ASN	New Anchor PC ASN notifies Relay Serving ASN of PC relocation. Serving ASN notifies MS.
$T_{R4\_PC\_Reloc\_Upd\_AA}$	New Anchor PC ASN	New 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.



#### 4.10.2.4.2 Authenticator Context Retrieval failure

Whenever the RNG-REQ authentication fails either because the CMAC is determined to be invalid or the Anchor Authenticator could not provide complete AK context, the ASN of the Relay PC SHALL instruct the MS to begin the “Un-secure Location Update”. Just as with failure of Secure Location Update, Unsecure Location Update is performed as MS network re-entry from Idle Mode process (see 4.10.2.4.4).

#### 4.10.2.4.3 PC Relocation Failure

PC Failure may occur if the Current Anchor PC ASN rejects PC relocation or a candidate Anchor PC rejects the *Relocation\_Req*. If PC relocation failure occurs for any reason, the current Anchor PC ASN SHALL continue to support the Anchor PC function and the serving ASN SHALL be notified by means of the R4 *LU\_Cnf* message.

If PC relocation requested by the Current Anchor PC ASN is refused because of failure or policy, then the Current Anchor PC MAY still release the context of the user due, for example, to overflowing of the LR database.

If PC relocation requested by the New Anchor PC ASN is refused, then the New Anchor PC MAY force the MS to perform Unsecure LU.

#### 4.10.2.4.4 Secure Location Update Failure

The Anchor PC receiving *LU\_Cnf* message including Failure indication TLV with an error code = Location Update Failure (0x37) should keep the MS information unchanged as if the LU Update procedure had not occurred.

MS receiving RNG-RSP message with “Failure of Idle Mode Location Update” should perform a network re-entry process (see 4.10.4). The network will re-authenticate the MS during network re-entry from Idle Mode. If the re-authentication still fails, any entity of the network which has kept any information related to the MS should not be changed.

If MS performs a network re-entry process caused by un-secure LU, not power down, after successful re-authentication with complete or optimized network re-entry, the Idle Mode Entry procedure may be initiated by MS or network as described in section 5.3.2.373.

If MS performs a network re-entry process caused by un-secure LU, power down request, after successful re-authentication with complete or optimized network re-entry, the MS or network should send DREG REQ/CMD to finish its power down process.

#### 4.10.2.4.5 CMAC Key Count Update Failure

If the R4 *CMAC Key Count Update* procedure fails then Anchor PC ASN Shall page the MS with cause code set to 02 (Network Re-Entry).

#### 4.10.2.4.6 Location Update out of MS Reattachment Zone

If the MS mobility access classifier is fixed or nomadic, the Anchor PC and the Authenticator SHALL check if the Serving BS ID belongs to the MS Reattachment Zone.

If the MS’ mobility access classifier is fixed or nomadic, the MS’ Authenticator will reject AK context requests for the unauthorized BS based on Authenticator’s knowledge of MS Reattachment Zone list. To reject the AK context request, the MS’ Authenticator responds to Anchor PC with Context-Rpt message that includes appropriate Failure Indication value and excludes MS’ AK context.

If the Serving BS ID does not belong to the MS Reattachment Zone or AK context retrieval has been rejected by the Authenticator, the Anchor PC sends R4 *LU Rsp* message back to the Serving ASN with Failure Indication; After that, the Serving BS sends *RNG RSP* message back to MS setting Location Update Response TLV value as 0x01(Failure of Location Update) and directing the MS to do initial network entry.

#### 4.10.2.5 Location Update Message Tables

**Table 4-153 – LU\_Req Primitive Structure**

IE	Description	M/O	Notes
BS Info	5.3.2.26	M	
> BS ID	5.3.2.25	M	BS ID indicating the BS where MS performs location update.
Paging Information	5.3.2.119	M	Paging Information TLV contains PAGING_CYCLE, PAGING_OFFSET, PAGING_INTERVAL_LENGTH, and Paging Group ID. The BS may make a suggestion for Paging Cycle and Paging Offset for the MS performing LU.
> Paging Cycle	5.3.2.118	O	
> Paging Offset	5.3.2.120	O	
> Paging Interval Length	5.3.2.135	O	
> Paging Group ID	5.3.2.123	O	
>Anchor PC ID	5.3.2.12	M	“PC ID” field in DREG_REQ on R1 points to MS’s anchor Paging Controller.
>Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS in Idle Mode, to be stored in Location Register during Location Update procedure.
>Anchor PC Relocation Destination	5.3.2.13	O	Identifier for destination Anchor PC in the event of Anchor PC relocation.
Network Exit Indicator	5.3.2.109	O	This is in case the LU is caused by Power Down Update.

**Table 4-154 – LU\_Rsp Primitive Structure**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	This SHALL be mandatory in the event there is a failure due unavailability of Authenticator or if present in Context Rpt. Presence of error code = 0x37 SHALL mean Location Update has failed.
BS Info	5.3.2.26	M	
> BS ID	5.3.2.25	M	BS ID indicating the BS where MS performs location update.
> AK Context	5.3.2.6	O	Security context required for BS to validate the received RNG-REQ message from MS and respond with RNG-RSP signed by a valid HMAC/CMAC digest.
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
MS Info	5.3.2.103	O	MS Info to be included in the event of PC relocation.
> Authenticator ID	5.3.2.19	O	
>Anchor ASN GW ID	5.3.2.10	O	This is included if PC Relocation Request has been accepted or is being requested.
>Mobility Access Classifier	5.3.2.423	O	Included if PC Relocation Request has been accepted or is being requested.
>Reattachment Zone	5.3.2.424	O	Included if PC Relocation Request has been accepted or is being requested.
Paging Information	5.3.2.119	O	Paging Information TLV contains PAGING_CYCLE, PAGING_OFFSET, PAGING_INTERVAL_LENGTH and Paging Group ID.
>Paging Cycle	5.3.2.118	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Offset	5.3.2.120	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Interval Length	5.3.2.135	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Group ID	5.3.2.123	O	
> Old Anchor PC ID	5.3.2.113	O	This TLV is included in the event of PC relocation.
> Anchor PC ID	5.3.2.12	O	This TLV is included in the event of PC relocation.
>Anchor PC Relocation Request Response	5.3.2.14	O	“Accept” or “Refuse”. Included only if PC Relocation is requested in R4 LU_Req
>Location Update Status	5.3.2.88	O	Shall be included if location update was successful, and SHALL not be included otherwise. If location update was refused or failure occurred, this is indicated by inclusion of the Failure Indication TLV.
PC Relocation Indication	5.3.2.122	O	Included by the Current Anchor PC to request PC relocation is included only in R4 LU_Rsp.

1

**Table 4-155 – LU\_Cnf Primitive Structure**

IE	Description	M/O	Notes
Failure Indication	5.3.2.69	O	Location Update Failure code SHALL be included.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the BS where MS performs location update.
> Serving/Target Indicator	5.3.2.182	M	Set to “Serving” if location update is a success else set to “Target”. Shall be included only in R4 <i>LU_Cnf</i>
MS Info	5.3.2.103	O	
> CMAC_Key_COUNT	5.3.2.34	M	Includes BS value of CMAC_KEY_COUNT to update an Authenticator.
Paging Information	5.3.2.119	O	The BS SHALL reflect the Paging Cycle, Paging Offset, Paging Interval Length and Paging Group Id received in the LU_Rsp.
>Paging Cycle	5.3.2.118	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Offset	5.3.2.120	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Interval Length	5.3.2.135	O	Anchor PC SHALL include this if BS had included a suggestion for this TLV.
>Paging Group ID	5.3.2.123	O	
>Anchor PC ID	5.3.2.12	O	Included if PC relocation was requested earlier.
>Relocation Success Indicator	5.3.2.149	O	Success if Relocation was accepted by destination and completed.

2

**Table 4-156 – Context\_Req Primitive Structure**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	
BS Info	5.3.2.26	M	Serving BS.
>BS ID	5.3.2.25	M	The BSID received in the R4 LU.
Paging Information	5.3.2.119	O	
>Anchor PC Relocation Destination	5.3.2.13	O	Identifier for destination Anchor PC, included in the event of Anchor PC relocation.

3

**Table 4-157 – Context\_Rpt Primitive Structure**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Provide failure indication for this message.

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	
BS Info	5.3.2.26	M	Serving BS.
>BS ID	5.3.2.25	M	BSID received in the corresponding R4 Context Request.
>AK Context	5.3.2.6	M	
>>AK	5.3.2.5	M	
>>AK ID	5.3.2.7	M	
>>AK Lifetime	5.3.2.8	M	
>>AK SN	5.3.2.9	M	
>>CMAC_KEY_COUNT	5.3.2.34	M	

**Table 4-158 – PC\_Relocation\_Ind Primitive Structure**

IE	Reference	M/O	Notes
Anchor PC ID	5.3.2.12	M	Indicating the new Anchor PC ID.
LU Result Indicator	5.3.2.90	M	This SHALL be mandatory in the event there is a failure reported in LU_Rsp. Presence of error code = 0x37 SHALL mean Location Update has failed. Location update Result Indicator TLV SHALL be Included independently of the failure code.

**Table 4-159 – PC\_Relocation\_Ack Primitive Structure**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

### 4.10.3 Paging Procedure

Paging procedures i.e., the sending of the *Paging\_Announce* messages occur under several scenarios which include:

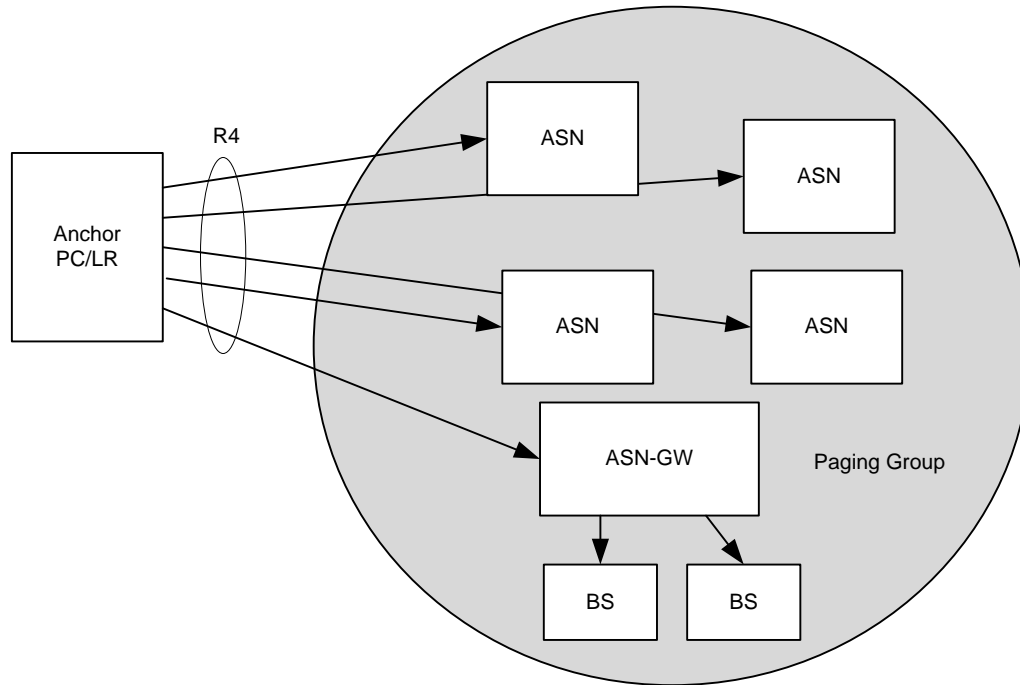
- Incoming data for the MS;
- Location update forced by the network for this MS;
- Network initiated MS network re-entry;
- Cancel *Paging\_Announce* once the MS has exited IDLE state.

Paging procedures may include topologically aware and unaware schemes.

Call flows described in this section may only occur when functional entities such as Relay PC, FA/ADPF, Anchor PC, and authenticator are located in different ASNs per each MS. If two functional entities shown are co-located in a single ASN the corresponding R4 signaling described are not exposed. For example, if the PC and Authenticator are collocated for an MS, R4 signaling between the PC and Authenticator are not exposed. Another example is that if the PC and FA/ADPF is located within a single ASN, the corresponding R4 signaling between the PC and FA is not exposed.

#### 4.10.3.1 Topologically Aware Paging

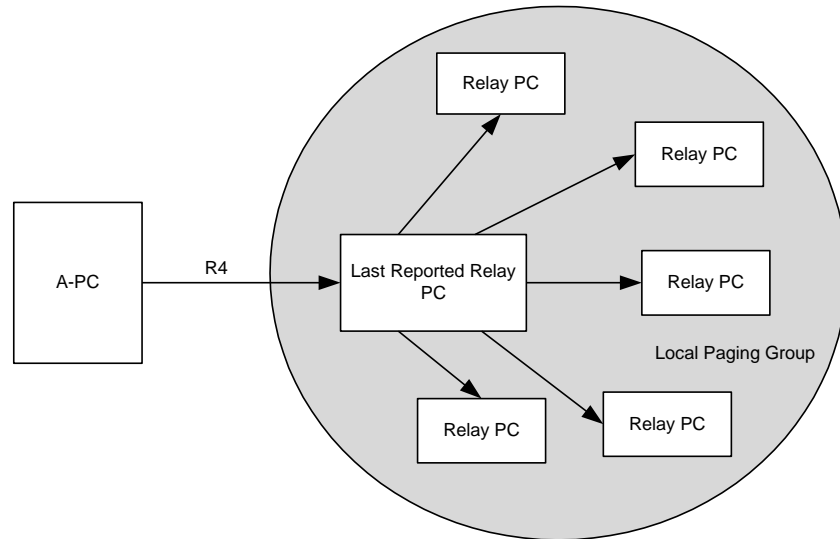
In the topologically aware paging scheme, the Anchor PC is aware of the Paging group's structure and contains the addresses of all the Relay-PC identities. In addition the PC may keep track of the BSID where the MS last performed a location update, and also neighboring BS topology to allow for multi-step paging. The Anchor PC directly sends R4 *Paging\_Announce* messages to only the Relay PCs associated with the MSs current PGID (see Figure 4-153). The Relay PC in turn will do single or multi-step paging based on the information contained in the received *Paging\_Announce* message. Topologically aware paging is an optional procedure for WiMAX networks.



**Figure 4-153 – Topologically Aware Paging Announce Scheme**

#### 4.10.3.2 Topologically Unaware Paging Scheme

In the topologically unaware paging scheme the Anchor PC is unaware of the topology or structure of the paging groups and has no knowledge of the paging group members associated with the PC-Relays that manage the various paging groups. As such several vendor specific paging schemes can be supported (e.g., flood paging where the Anchor PC sends a message to all associated Relay PC's). The following describes an example of a topologically unaware paging procedure (see Figure 4-154). The Anchor PC keeps track of the Relay PC, reported by the last Location Update message received from the MS. As the MS in Idle Mode traverses the network, it performs location updates as it passes through different paging groups. The Anchor PC/LR keeps updating the last reported Relay PC so that a *Paging\_Announce* message can be forwarded to it when the MS is paged. The last reported Relay PC (i.e., the local PC), is topologically aware and maintains the list of its local neighboring ASNs and additional Relay PCs that are part of the Paging group and forwards the *Paging\_Announce* message to the paging group members as well as the BSs under its control. The additional Relay PC will in turn forward the *Paging\_Announce* message to the BS their control. The topologically unaware Anchor PC relies on the last reported Relay PC, to contain the list of pertinent Base Stations and/or Relay PCs that need to be paged. This list is defined by the network operator and is based on the local topology of a group of neighboring Base Stations within the same paging group. Note that for optimization, the member list may also include neighboring Base Stations that belong to adjacent page groups that may be deemed appropriate for paging as well. Topologically unaware paging is a mandatory procedure for WiMAX networks.



**Figure 4-154 – Topologically Unaware Paging Announce Scheme**

#### 4.10.3.3 Single-step vs. Multi-step Paging Operations

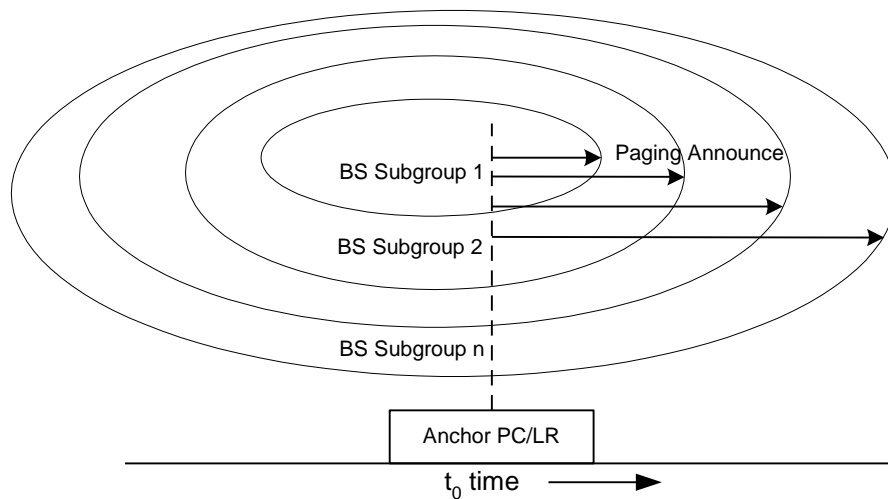
For efficiency and flexibility in the implementation of paging operation, paging may be performed in a single step or multiple steps. The following provides illustrative examples of single and multi-step Paging Announce algorithm.

##### Single-step Operation:

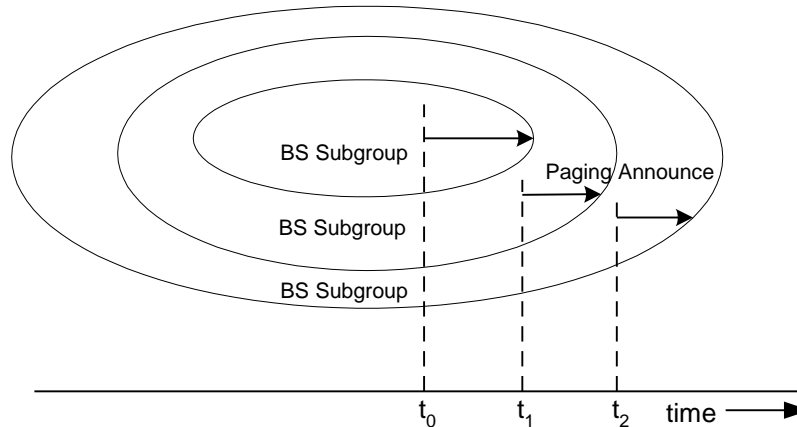
In a single step paging operation, when a MS is to be paged, the PC/LR directly sends *Paging\_Announce* messages to each Relay PC in the list defined for the paging group last reported by the MS. The Local/Relay PC directly sends *Paging\_Announce* messages to each Base Station in the BS ID IE if received 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.



**Figure 4-155 – Single-step Paging**



**Figure 4-156 – Multi-step Paging**

#### 4.10.3.4 IP Multicasting Support for Paging\_Announce

IP Multicasting [22] MAY be used for announcing the paging information for an Idle Mode MS or a set of Idle Mode MS's via the *Paging\_Announce* message.

Multicast groups may be created as described in [22]. Each multicast group contains some set of the BSs – the exact grouping being implementation dependent.

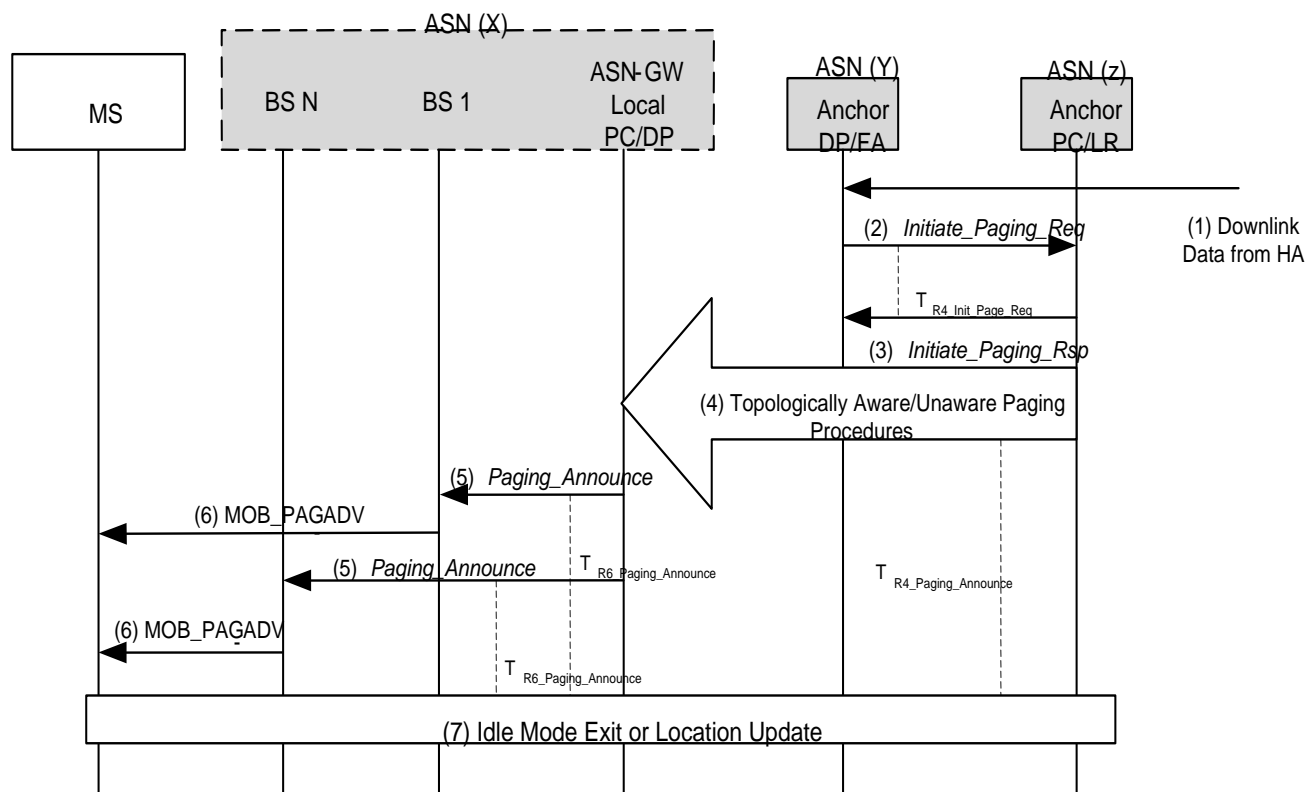
Each multicast group is assigned a multicast IP address, which is used as the destination address in the IP header of the *Paging\_Announce* message.

In general, non-members of the group can also receive the message sent using multicast IP address. However, only the members of the group can be recipients of the messages sent to the group.

#### 4.10.3.5 Paging Procedure Message Flow

The following call flow illustrates the paging procedure. The paging operation can be triggered by several actions, but the paging procedure for each trigger is similar. Figure 4-157 illustrates the paging procedure triggered by DL data arrival for a MS when the MS is in Idle Mode.





**Figure 4-157 – Paging Procedure**

#### STEP 1

Data from HA arrives through the tunnel at the FA and its associated DPF. The Anchor DPF buffers the data.

#### STEP 2

The Anchor Data Path Function determines that MS is in Idle Mode and SHALL activate it before the received data can be delivered. Anchor DPF sends an R4 *Initiate\_Paging\_Req* message to Anchor PC/LR to request paging. Optionally the R4 *Initiate\_Paging\_Req* message contains the QoS parameters of the flow for which the data arrived at the Anchor DPF. This helps set priority treatment of the Paging operation based on the QoS parameters and flow types. The Anchor DPF may have policies for triggering paging based on the QoS parameters for the data received. The Anchor DP Function starts timer  $T_{Init\_Page\_Req}$ .

Note: When MS is in Idle Mode, if data not belonging to any saved SF of the MS arrives, the decision to initiate paging or not is left for operator's setting.

#### STEP 3

Anchor PC/LR retrieves the information related to the MS and sends an R4 *Initiate\_Paging\_Rsp* to Anchor Data Path function. This message is used to indicate whether the MS context as contained in the PC/LR is correct and the requested paging action is authorized. Exclusion of the Response Code TLV indicates intent to page the MS. Upon receipt of this message the Anchor DP Function stops timer  $T_{Init\_Page\_Req}$  if running.

#### STEP 4

If paging action is authorized, Anchor PC retrieves the MS paging information and constructs *Paging\_Announce* message. The Anchor PC MAY issue one or more *Paging\_Announce* messages based on its knowledge of the

Paging Region topology as shown in sections 4.10.3.1 and 4.10.3.2. The Anchor PC MAY issue *Paging\_Announce* message(s) to the appropriate Relay PC(s) or directly to BS(s), according to its knowledge of the Paging Region topology. The Anchor PC SHOULD start a timer  $T_{R4\_Paging\_Announce}$  when it sends out the first *Paging\_Announce* message and SHOULD wait for the paging response. The Anchor PC MAY set a paging re-transmission counter N and - until exhausting the re-transmission counter, and until a paging response is received at the Anchor PC does not receive a paging response—may retransmit the *Paging\_Announce* message prior to the expiration of the timer  $T_{R4\_Paging\_Announce}$ . If re-transmitted, the *Paging\_Announce* message SHALL be sent no more than N times before the expiration of timer  $T_{R4\_Paging\_Announce}$ .

If the Anchor PC is topologically aware of the defined Paging Group (PG), including the last BS from which the MS performed location update, the Anchor PC SHALL directly issue *Paging\_Announce* messages to all, or some subset, of the Paging Group members consisting of BSs and/or relay PCs in the region.

If the Anchor PC is topologically unaware of the Paging region, or the BSs defined in the Paging group, but rather one or more Relay PCs, the *Paging\_Announce* messages are sent to the known Relay PC(s). The Relay PC(s) then appropriately forwards the announce message to all the one or more BSs in the Paging region.

If the MS mobility access classifier is fixed or nomadic, the Anchor PC should use the MS reattachment zone to optimize paging. For topology-unaware scheme, Anchor PC should include the BSIDs of the BSs that belong to the MS Reattachment zone in the *Paging\_Announce* message.

#### STEP 5

The ASN-GW that contains the local/relay PC function for the MS initiates the paging operation and sends the R6 *Paging\_Announce* message to the relevant BS(s) associated with the PGID received in R4 *Paging\_Announce* both for the original and re-transmitted R4 *Paging\_Announce*. The ASN GW may perform single step or multi-step paging as described in section 4.10.3.3 based on if BS ID TLV or the L-BSID TLV is present. Associated with each R4 *Paging\_Announce* message the ASN-GW containing local/relay PC starts timer  $T_{R6\_Paging\_Announce}$  and reset it when R6 *Paging\_Announce* is re-transmitted in response to the reception of re-transmitted R4 *Paging\_Announce* message.

#### STEP 6

Once the Paging Agent (PA) at the BS receives the *Paging\_Announce* message with the requested action set to “Start” it extracts the relevant paging parameters for the MS (Paging Cycle, Paging Offset) and initiates the paging action requested by sending out MOB-PAG\_ADV message over the airlink as per the indicated paging cycle and the paging offset. When the message is sent in response to downlink data being received for the MS, the Action Code in the message is set to 0b10 (Enter Network). When the message is sent to trigger a location update from the MS, the Action Code in the message is set to 0b01 (Perform Ranging to establish location and acknowledge message). See IEEE 802.16e section 6.3.2.3.56. The optional SF Flow info in the message helps the BS implement a paging priority scheme for faster call setup when bandwidth is constrained or for resource allocation. The PA will continue to page the MS for the duration specified by the Paging Announce Timer TLV or until the appropriate response is received from the MS or a stop page indication is received from the Local PC.

#### STEP 7

Upon being successfully paged the MS will perform an Idle Mode Exit or a Location Update procedure. If any Paging Agent (PA) receives a successful reply from the paged MS, the Paging Agent will notify the Local PC by sending an R6 *LU\_Req* message in the case of Network Initiated location update or R6 *IM\_Exit\_State\_Change\_Req* message in the case of data delivery to MS in idle mode. Upon receipt of a such a message the Local PC will stop timer  $T_{R6\_Paging\_Announce}$  if running, and in turn will send the appropriate R4 *LU\_Req* or R4 *IM\_Exit\_State\_Change\_Req* message to the Anchor PC. Upon receipt of such a message, the Anchor PC will stop timer  $T_{R4\_Paging\_Announce}$ , if running. The Anchor PC may also initiate stop paging procedures (see 4.10.3.6).

#### 4.10.3.6 Stop Paging Procedure

The Paging stop operation is illustrated in Figure 4-158. It is assumed that the MS is being paged over multiple BSs (this could be triggered for example either in response to incoming data to be delivered to the MS or network initiated location update. See section 4.10.3 for detail on the paging process). Upon the PC detecting a response

from the MS (e.g., receipt of *LU\_Req* or *IM\_Exit\_State\_Change\_Req*), the Anchor PC may send a *Paging\_Announce* message with paging start/stop=0 to alert all BSs to stop the paging procedure. This Stop Paging process is a method to prematurely end the normally timed Paging Advertisement method. The support of the Stop Paging procedure is optional.

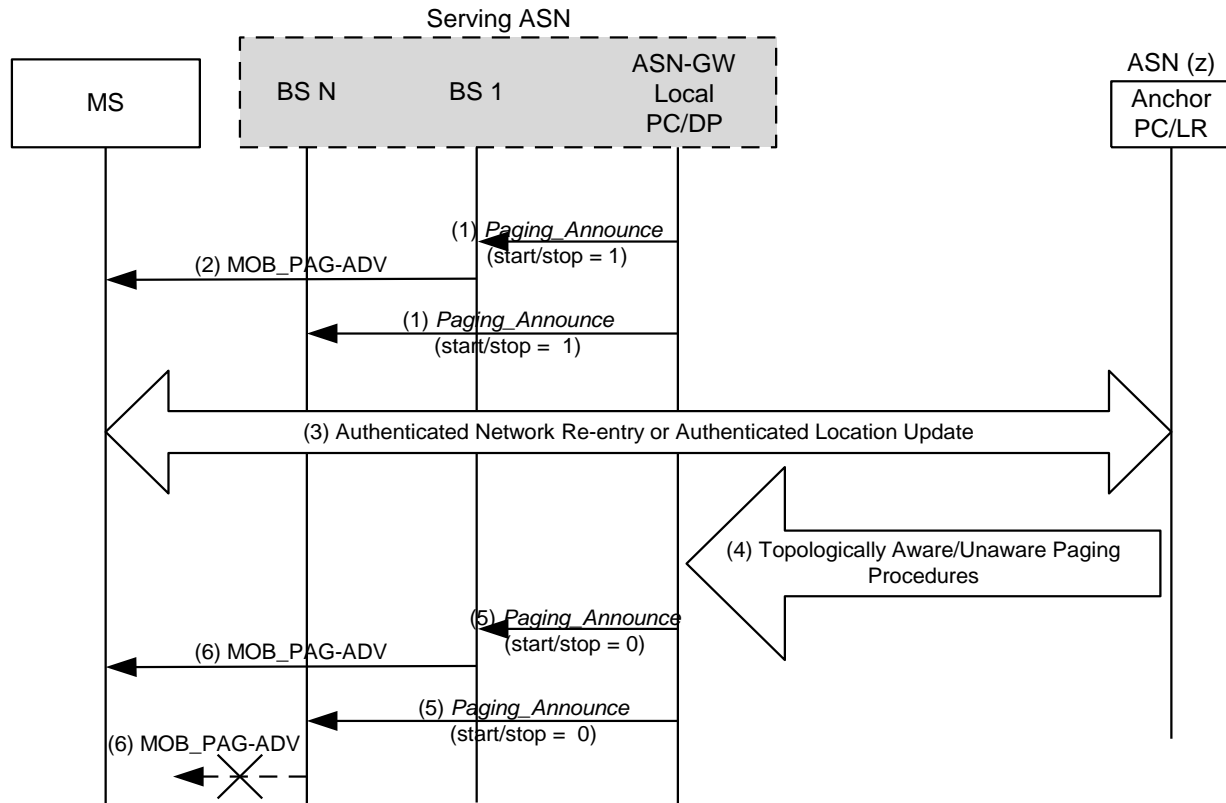


Figure 4-158 – Stop Paging Procedure

#### 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 *LU\_Req* or *IM\_Exit\_State\_Change\_Req* 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.

If the MS mobility access classifier is fixed or nomadic, the Anchor PC should use the MS Reattachment Zone to optimize paging. For topology-unaware scheme, Anchor PC should include the BS IDs of the BSs that belong to the MS Reattachment zone in the *Paging\_Announce* message.

#### 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

Once the Paging Agent (PA) at the BS receives the *Paging\_Announce* message with the requested action set to “Start”, it extracts the relevant paging parameters for the MS (Paging Cycle, Paging Offset) and initiates the paging action requested by sending out MOB-PAG\_ADV message over the air link as per the indicated paging cycle and the paging offset. When the message is sent in response to downlink data being received for the MS, the Action Code in the message is set to 0b10 (Enter Network). When the message is sent to trigger a location update from the MS, the Action Code in the message is set to 0b01 (Perform Ranging to establish location and acknowledge message). See IEEE 802.16e section 6.3.2.3.56. The optional SF Flow info in the message helps the BS implement a paging priority scheme for faster call setup when bandwidth is constrained or for resource allocation. The Paging Agent will continue paging the MS for the duration specified by the Paging Announce Timer TLV, or until the appropriate response is received from the MS, or until it receives a Paging::Stop message for the MS from the Paging Controller, or the Paging Agent’s internal paging timer value expires, or an implementation-specific algorithm decides to stop the paging – whichever comes first.

#### 4.10.3.7 Paging Timers and Timing Considerations

This section identifies the timer entities participating in the Paging procedure. The following timers are defined over R4 and R6:

- $T_{R4\_Paging\_Announce}$ : is started by the Anchor PC/Relay upon sending a R4 *Paging\_Announce* message. It is stopped upon receiving R4 *LU\_Req* or R4 *IM\_Exit\_State\_Change\_Req* message.
- $T_{R6\_Paging\_Announce}$ : is started by the Local PC/Relay PC upon sending a R6 *Paging\_Announce* message. It is stopped upon receiving R6 *LU\_Req* or R6 *IM\_Exit\_State\_Change\_Req* message.
- $T_{R4\_Init\_Page\_Req}$ : is started by the Anchor DP function upon sending the R4 *Initiate\_Paging\_Req* message to the Anchor PC, and is stopped upon receiving a corresponding the R4 *Initiate\_Paging\_Rsp* message.

Table 4-160 shows the default value of timers and also indicates the range of the recommended duration of these timers. Note that these values are provisioned in the current Release.

**Table 4-160 – 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

#### 4.10.3.8 Paging Error Conditions

This section describes error conditions associated with the Paging Procedure.

##### 4.10.3.8.1 Timer Expiry

Table 4-161 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer expiry, if the maximum retries has not exceeded, the timer is restarted.

**Table 4-161 – Timer Max Retry Conditions**

Timer	Entity where Timer Started	Action(s)
T <sub>R4_Paging_Announce</sub>	Anchor PC / Relay PC	The Anchor PC SHALL consider the MS unavailable and stop paging. The Relay PC has no action.
T <sub>R6_Paging_Announce</sub>	Relay PC / Local PC	No action.
T <sub>R4_Init_Page_Req</sub>	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.

#### 4.10.3.8.2 R4 Initiate\_Paging\_Rsp

Upon receipt of the R4 *Initiate\_Paging\_Req* message, if the Anchor PC is unable to initiate paging procedures for the MS, it SHALL send a R4 *Initiate\_Paging\_Rsp* message and include the Response Code TLV with suitable error code value. Upon receipt of R4 *Initiate\_Paging\_Rsp* message indicating that paging cannot be initiated for the MS, the Anchor DP function MAY resend the R4 *Initiate\_Paging\_Req* message. If the Anchor DP function does not resend the R4 *Initiate\_Paging\_Req* message or if the subsequent attempts are also unsuccessful, then 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.

#### 4.10.3.9 Messages for Paging Procedure

This section provides the message definitions for the R4 and R6 messages in support of the Paging procedure. See also sections 5.2 and 5.3 for message and TLV definitions respectively.

**Table 4-162 – R4 Initiate\_Paging\_Req**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	O	
>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.
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.

**Table 4-163 – R4 Initiate\_Paging\_Rsp**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

Response Code	5.3.2.153	O	Included in paging not allowed. Valid values: <ul style="list-style-type: none"> <li>0x00 = Not allowed - Paging Reference is zero</li> <li>0x01 = Not allowed - No such SF</li> </ul>
---------------	-----------	---	--

1

**Table 4-164 – R4 Paging\_Announce**

IE	Reference	M/O	Notes
BS Info	5.3.2.26	O	
>Reattachment Zone	5.3.2.424	O	Included if the MS mobility access classifier is fixed or nomadic.
>BS ID(s)	5.3.2.25	CM	When included, the paging SHALL only be executed at the base stations identified by the BS ID(s) for multi-step paging procedure. 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.
Paging Information	5.3.2.119	M	Paging Information TLV obtained from the MS containing PAGING_CYCLE, PAGING_OFFSET, PAGING_INTERVAL_LENGTH and Paging Group ID. This IE is included for Paging (start) operation; however it is not required for Paging stop.
>Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS to be paged which was last stored in Location Register.
>Paging Start/Stop	5.3.2.121	M	1 = start Paging Operation. 0 = stop Paging Operation.
>Paging Announce Timer	0	O	This IE is included for Paging (start) operation. This is not included for paging stop operation.
> Paging Cycle	5.3.2.118	O	This SHALL be mandatory when Paging. Start/Stop = 1.
> Paging Offset	5.3.2.120	O	This SHALL be mandatory when Paging. Start/Stop = 1.
> Paging Interval Length	5.3.2.135	O	This SHALL be mandatory when Paging. Start/Stop = 1.
> Paging Group Id	5.3.2.123	M	This is mandatory if the L-BSID and BSID(s) are not present.
>Paging Cause	5.3.2.116	O	01 = Location update. 02 = Network Re-Entry, Incoming Data for Idle

IE	Reference	M/O	Notes
			MS. Other values are reserved. This SHALL be mandatory when Paging Start/Stop = 1.
> Anchor PC ID	5.3.2.12	O	
MS Info	5.3.2.103	O	
> 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.
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.
> Authenticator ID	5.3.2.19	O	Included as an optimization for reducing the Network entry latency.

1

**Table 4-165 – R6 Paging\_Announce**

IE	Reference	M/O	Notes
MS Info	5.3.2.103	O	
> SF Info	5.3.2.185	O	SF Flow Info for preferential treatment for paging and call origination. This is not included for paging stop operation.
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.
> Authenticator ID	5.3.2.19	O	Included if received in the R4 Paging_Announce message.
Paging Information	5.3.2.119	M	This compound TLV contains Paging Cycle, Paging Offset, PAGING_INTERVAL_LENGTH and PG ID. This IE is included for Paging operation.
>Anchor PC ID	5.3.2.12	O	Included if received in the R4 <i>Paging_Announce</i> message.
>Paging Start/Stop	5.3.2.121	M	1 = start Paging Operation. 0 = stop Paging Operation.
>Paging Announce Timer	0	O	This IE is included for Paging (start) operation. This is not included for paging stop operation.
> Paging Cycle	5.3.2.118	O	This SHALL be mandatory when Paging. Start/Stop = 1.
> Paging Offset	5.3.2.120	O	This IE is included for Paging (start) operation.

IE	Reference	M/O	Notes
			This is not included for paging stop operation.
> Paging Interval Length	5.3.2.135	O	This SHALL be mandatory when Paging. Start/Stop = 1.
> Paging Group Id	5.3.2.123	M	This IE is included for Paging (start) operation. This is not included for paging stop operation.
>Paging Cause	5.3.2.116	O	01 = Location update. 02 = Network Re-Entry, Incoming Data for Idle MS. Other values are reserved. This SHALL be mandatory when Paging Start/Stop = 1.

1



## 4.10.4 Idle Mode Exit

### 4.10.4.1 Idle Mode Exit – Serving ASN Does Not Have MS Context

The call flow for a typical scenario for the MS exiting idle mode is shown below. Here it is assumed that when the MS is trying to re-enter the network from idle mode, (i.e., exit the idle mode), the serving ASN does not have any context for this MS – hence, the entire context has to be retrieved from the Anchor PC. In other words the MS tries to re-enter the network when the “management resource holding timer” has expired in the network. Section 4.10.4.2 describes the idle mode exit procedure before the expiry of the Management Resource Holding Timer.

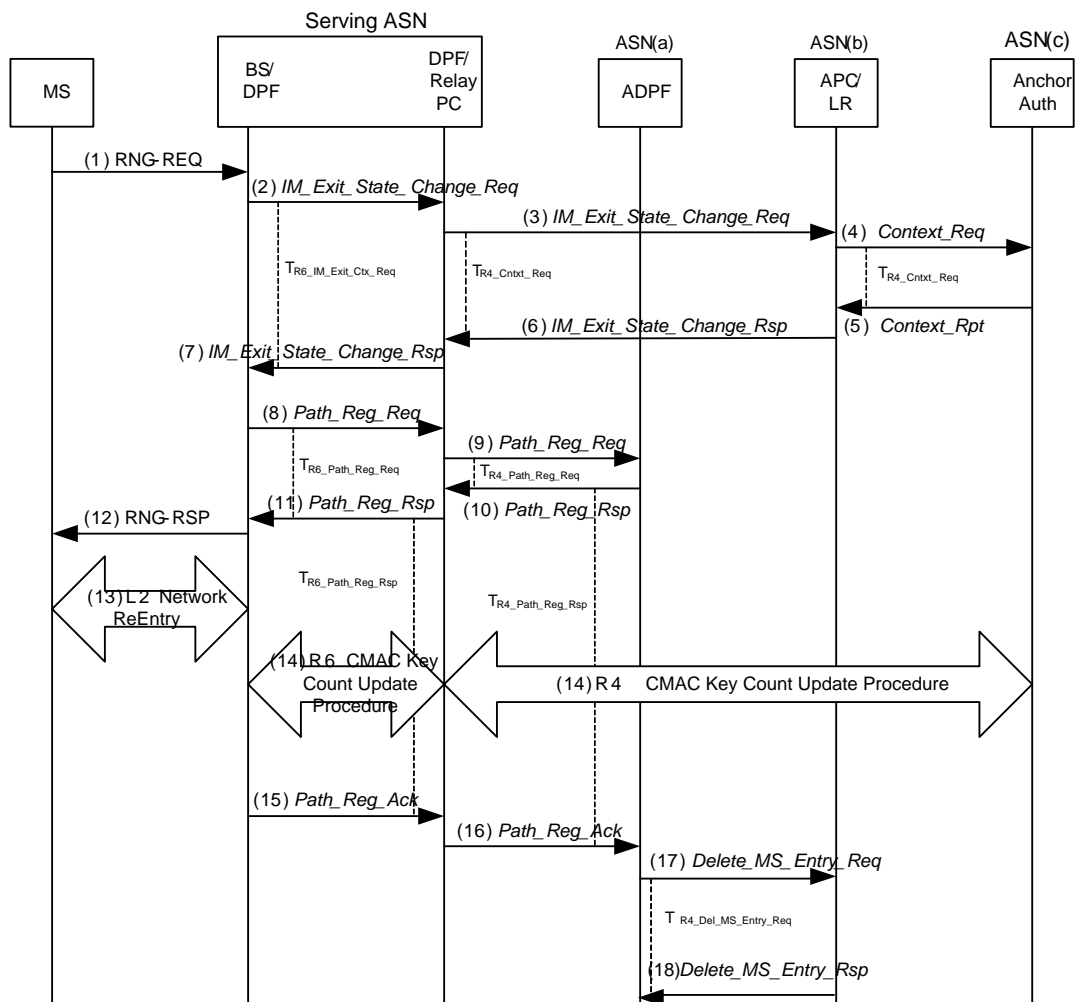


Figure 4-159 – Idle Mode Exit Procedure

#### Flow Description

MS CAN exit Idle mode in two ways, initiated by the network through Paging or on its own becomes active so that it can communicate. Though the steps in the two scenarios are the same, the sequences are different and some of the steps could be optional.

#### Case a: Network initiated Idle mode exit (in response to a page)

When MS exits Idle mode in response to a prior Page message, it performs Ranging (RNG\_REQ).

**Case b: MS initiated Idle mode exit**

When MS on its own wants to become active to initiate communication, it performs the steps given below.

**STEP 1**

MS initiates exit procedure from IDLE mode and sends RNG\_REQ as described in IEEE 802.16 specification. The Ranging Purpose Indication TLV Bit #0 is set to one and PC ID TLV is included, thus indicating that the MS intends to Re-Entry from Idle Mode.

**STEP 2**

The BS receives the RNG\_REQ message from MS indicating Idle mode exit and sends R6 *IM\_Exit\_State\_Change\_Req* to the Relay PC in the ASN-GW, indicating that the MS wants to become active. Timer  $T_{R6\_IM\_Exit\_Ctx\_Req}$  is started at this point by the BS to monitor the response for this message.

**STEP 3**

The Relay PC in the Serving ASN receives the R6 *IM\_Exit\_State\_Change\_Req* from the BS indicating Idle mode exit and sends R4 *IM\_Exit\_State\_Change\_Req* to the Anchor PC/LR in ASN(b), indicating that the MS wants to become active. In the event that the relay PC is the anchor PC, this step is not required.

If the MS mobility access classifier is fixed or nomadic, the Anchor PC SHALL check whether the Serving BS ID belongs to the MS Reattachment Zone. Only if the Serving BS ID belongs to the MS Reattachment Zone, the Anchor PC proceeds with step 4, otherwise it proceeds with step 6 to direct the MS to do initial network entry.

**STEP 4**

On receiving the R4 *IM\_Exit\_State\_Change\_Req*, the Anchor PC/LR proceeds to request the security context from the Anchor Authenticator in ASN(c) using the R4 *Context\_Req*. Timer  $T_{R4\_Cntxt\_Req}$  is started at this point by the Anchor PC to monitor the response for this message. This step is optional if the Anchor Authenticator and Anchor PC/LR are co-located in the same gateway.

**STEP 5**

Anchor Authenticator responds with the security context back to the Anchor PC/LR with R4 *Context\_Rpt* message. Once the Anchor PC receives this message, Timer  $T_{R4\_Cntxt\_Req}$  is stopped. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN.

**STEP 6**

Anchor PC/LR, sends R4 *IM\_Exit\_State\_Change\_Rsp* to the Relay PC. R4 *IM\_Exit\_State\_Change\_Rsp* contains the stored information for the MS at the Anchor PC.

**STEP 7**

Serving ASN retrieves the MS context from Anchor PC ASN and forwards the MS context to the BS on the R6 interface. Once the BS receives this message, Timer  $T_{R6\_IM\_Exit\_Ctx\_Req}$  is stopped. The message is defined in section 5.2. The AK fetched from the authenticator is used to verify the RNG-REQ.

**STEP 8**

After successful authentication, the BS starts data path establishment – it sends R6 *Path\_Reg\_Req* to the DPF in the serving ASN. Timer  $T_{R6\_Path\_Reg\_Req}$  is started at this point by the BS to monitor the response for this message.

**STEP 9**

The Serving ASN extends the data path establishment to the FA or Anchor DPF in ASN(a) across the R4 interfaces.

**STEP 10**

The Data Path Function associated with FA or A\_DPF in ASN(a) confirms data path establishment and sends R4 *Path\_Reg\_Rsp* back to the Serving ASN. Timer  $T_{R4\_Path\_Reg\_Rsp}$  is started at this point by the Anchor DPF to monitor the ACK for this message.

**STEP 11**

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

**STEP 12**

The BS will use MS service and operational information indicated by IDLE Mode Retain Info obtained by Step 7 to construct HO Process Optimization TLV (802.16e parameter) settings in the RNG-RSP based on local policy; then sends RNG\_RSP message to the MS formatted according to IEEE 802.16e specification. This message delivers all the required information to resume service in accordance with Idle Mode Retain Information.

**STEP 13**

The MS completes Network Re-Entry from the Idle Mode as described in IEEE 802.16e specification. Acknowledge to the Data Path function in the serving ASN confirming intra-ASN data path establishment completion and service flows establishment.

**STEP 14**

The BS updates the Anchor Authenticator with the CMAC Key count for the MS via the serving ASN. It includes the Idle Mode Exit Indicator TLV in the CMAC\_Key\_Count\_Update\_Req. The procedure for this operation is described in section 4.12. The Anchor Authenticator acknowledges the CMAC update for the MS.

**STEP 15**

Upon the MS Network Re-Entry completion the BS sends R6 *Path\_Reg\_Ack* to the data path function in the serving ASN.

**STEP 16**

The Data Path function in serving ASN sends an inter-ASN R4 *Path\_Reg\_Ack* to the Data Path function associated with Anchor DPF/FA. Timer  $T_{R4\_Path\_Reg\_Rsp}$  is stopped at the anchor DPF.

**STEP 17**

When R4 *Path\_Reg\_Ack* is received at Anchor DPF, the Data Path function associated with FA sends a R4 *Delete\_MS\_Entry\_Req* message to PC/LR in order to delete the Idle mode entry associated with the MS. If MS is exiting Idle mode due to a network initiated Idle mode exit, the PC/LR will cease all Paging Announce operations. Timer  $T_{R4\_Del\_MS\_Entry\_Req}$  is started at this point by the Anchor DPF to monitor the response for this message. This step is optional if the Anchor DPF and Anchor PC/LR are co-located in the same gateway.

**STEP 18**

Upon the Anchor PC receives *Delete\_MS\_Entry\_Req*, Anchor PC sends *Delete\_MS\_Entry\_Rsp* to Anchor DPF.

Timer  $T_{R4\_Del\_MS\_Entry\_Req}$  is stopped at the Anchor DPF.

**4.10.4.1.1 Timers and Timing Considerations**

This section identifies the timer entities participating in the IM exit procedure. The IM exit procedure definition shown in Table 4-166 employs the following timers:

- $T_{R6\_IM\_Exit\_Ctx\_Req}$ : is started by a BS upon sending the R6 *IM\_Exit\_State\_Change\_Req* message to the relay PC in the ASN-GW. It is stopped upon receiving a corresponding response.

- $T_{R4Cntxt\_Req}$ : is started by an anchor PC entity upon sending the R4 *Context\_Req* message to the anchor authenticator. It is stopped upon receiving R4 *Context\_Rpt*.
- $T_{R6\_Path\_Reg\_Req}$ : is started by the BS upon sending the “R6 Path Registration REQ” message to the serving ASN DPF. It is stopped upon receiving R6 *Path\_Reg\_Rsp*.
- $T_{R4\_Path\_Reg\_Rsp}$ : is started by the Anchor DPF upon sending the “R4 *Path\_Reg\_Rsp*” message to the Serving ASN. It is stopped upon receiving a corresponding response.
- $T_{R4\_Del\_MS\_Entry\_Req}$ : is started by an Anchor DPF entity upon sending the R4 *Delete\_MS\_Entry\_Req* message to another Anchor PC/LR. It is stopped upon receiving the R4 *Delete\_MS\_Entry\_Rsp*.

Table 4-166 shows the default value of timers and also indicates the range of the recommended duration of these timers. Note that these values are provisioned in the current Release.

**Table 4-166 – 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
$T_{R4\_Cntxt\_Req}$	TBD		TBD
$T_{R6\_Path\_Reg\_Req}$	TBD		TBD
$T_{R4\_Path\_Reg\_Rsp}$	TBD		TBD
$T_{R4\_Del\_MS\_Entry\_Req}$	TBD		TBD

#### 4.10.4.1.2 Idle Mode Exit Error Conditions

This section describes error conditions associated with the IM exit procedure.

##### 4.10.4.1.2.1 Timer Max Retries

Table 4-167 shows details on the timer expiry causes, reset triggers and corresponding actions. Upon each timer expiry, if the maximum retries has not exceeded, the timer is restarted.

**Table 4-167 – 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.
$T_{R4Cntxt\_Req}$	Anchor PC	Anchor PC indicates to the Relay PC, failure of context retrieval for the MS in the <i>IM_Exit_State_Change_Rsp</i> message.
$T_{R6\_Path\_Reg\_Req}$	BS DPF	RNG-RSP message indicating that IM Exit is not possible is sent to the MS on the air interface.
$T_{R4\_Path\_Reg\_Rsp}$	ASN DPF	ASN DPF indicates to the downstream ASN DPF, the failure of data path setup for the MS in the R4 <i>Path_Reg_Rsp</i> message.
$T_{R4\_Del\_MS\_Entry\_Req}$	ASN DPF	No action required.

#### 4.10.4.1.2.2 AK Context Generation Error

The Anchor Authenticator generates AK and AK Context information upon receipt of the R4 *Context\_Req*. If the Anchor Authenticator is unable to generate this information, it sends the *Context\_Rpt* 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  $T_{IM\_Cntxt\_Req}$  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.

#### 4.10.4.1.2.5 Serving BS not in MS Reattachment Zone

If the MS mobility access classifier is fixed or nomadic, the Anchor PC and the Authenticator SHALL check if the Serving BS ID belongs to the MS Reattachment Zone.

If the MS' mobility access classifier is fixed or nomadic, the MS' Authenticator SHALL reject context requests retrieval for the unauthorized BS based on Authenticator's knowledge of MS Reattachment list. To reject the context request, the MS' Authenticator responds to Anchor PC with *Context-Rpt* message that includes appropriate Failure Indication value and excludes MS' AK context.

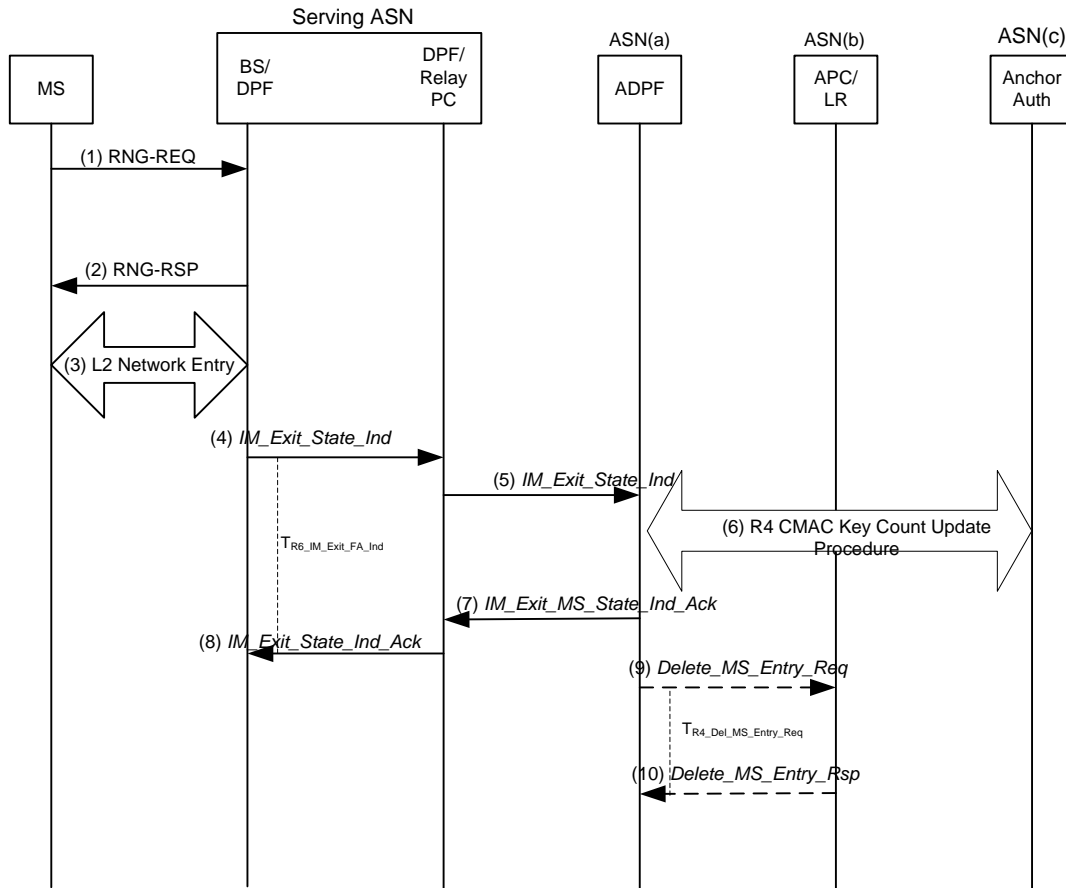
If the Serving BS ID does not belong to MS Reattachment Zone or context retrieval has been rejected by the Authenticator, then the Anchor PC sends the *IM\_Exit\_State\_Change\_Rsp* with the inclusion of the failure indication – thereby indicating that the Serving BS is out of MS Reattachment Zone. Then the BS will send the appropriate failure code to the MS on R1 via *RNG-RSP* message directing the MS to initial network entry.

#### 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. When located in the same ASN, the Anchor PC SHALL send a control message – R6 *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 4-160.



**Figure 4-160 – 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 an RNG-REQ to enter back into the network from Idle mode before the timer expires.

#### STEP 2

The BS has the required context now and the data paths retained for this MS since Management Resource Holding Timer is not expired. Hence it authenticates the MS and sends RNG-RSP back to the MS.

#### STEP 3

The MS completes Network Re-Entry from the Idle Mode as described in IEEE 802.16e specification.

#### STEP 4

The BS SHALL send R6 *IM\_Exit\_State\_Ind* to the DPF in the serving ASN-GW to indicate the MS exiting the idle mode before the timer expiry. It SHALL include the CMAC\_Key\_Count and Idle Mode Exit Indicator TLVs in the message in order to update the Anchor Authenticator. Timer *T<sub>R6\_IM\_Exit\_FA\_Ind</sub>* is started at this point by the BS to monitor the response for this message.

## STEP 5

The DPF in the serving ASN SHALL send the corresponding R4 *IM\_Exit\_State\_Ind* to the Anchor DPF in ASN(a) to indicate the MS exiting the idle mode before the Management Resource Holding Timer expiry.

## STEP 6

On receiving the R4 *IM\_Exit\_State\_Ind*, the Anchor DPF proceeds to inform the Anchor Authenticator in ASN(c). It includes the Idle Mode Exit Indicator TLV in the CMAC\_Key\_Count\_Update\_Req. The procedure for this is described in section 4.13. The Anchor Authenticator acknowledges the update. This step is optional if the Anchor Authenticator and Anchor DPF are co-located in the same gateway.

## STEP 7

The Anchor DPF in ASN(a) SHALL respond with R4 *IM\_Exit\_State\_Ind\_Ack* to the DPF in the serving ASN.

## STEP 8

The DPF in the serving ASN-GW SHALL forward the received message as R6 *IM\_Exit\_State\_Ind\_Ack* to the BS. Once the BS receives this message, timer  $T_{R6\_IM\_Exit\_FA\_Ind}$  is stopped.

## STEP 9

The Anchor DPF SHALL send the R4 *Delete\_MS\_Entry\_Req* to the Anchor PC in ASN(b), to remove the entry of this MS from the LR database in the anchor PC. It SHALL start timer  $T_{R4\_Del\_MS\_Entry\_Req}$ . This step is optional if the Anchor DPF and Anchor PC/LR are co-located in the same gateway.

## STEP 10

The APC/LR SHALL remove the entry for the MS from the LR database and send the R4 *Delete\_MS\_Entry\_Rsp* to the Anchor DPF in ASN(a). Upon reception, Anchor DPF SHALL stop the timer  $T_{R4\_Del\_MS\_Entry\_Req}$ .

### 4.10.4.2.1 Timers and Timing Considerations

This section identifies the timer entities participating in the IM exit procedure. The IM exit procedure definition shown in Table 4-168 employs the following timers:

- $T_{R6\_IM\_Exit\_FA\_Ind}$ : is started by a BS upon sending the R6 *IM\_Exit\_State\_Change\_Req* message to the serving DPF in the ASN-GW. It is stopped upon receiving a corresponding response.
- $T_{R4\_Del\_MS\_Entry\_Req}$ : is started by an Anchor DPF entity upon sending the R4 *Delete\_MS\_Entry\_Req* message to another Anchor PC/LR. It is stopped upon receiving the R4 *Delete\_MS\_Entry\_Rsp*.

Table 4-168 shows the default value of timers and also indicates the range of the recommended duration of these timers. Note that these values are provisioned in the current Release.

**Table 4-168 – 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
$T_{R4\_Del\_MS\_Entry\_Req}$	TBD		TBD

#### 4.10.4.2.2 Fast Idle Mode Exit Error Conditions

This section describes error conditions associated with the IM exit procedure.

##### 4.10.4.2.2.1 Timer Max Retries

Table 4-169 shows details on 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 4-169:

**Table 4-169 – 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.
$T_{R4\_Del\_MS\_Entry\_Req}$	Anchor ASN DPF	No action required.

##### 4.10.4.2.2.2 MS CMAC Validation Failure

In case, CMAC validation failure occurs at BS, it SHALL send the appropriate failure indication TLV in the RNG\_RSP to the MS. It SHALL then initiate Data Path tear down by sending Data Path Dereg Req.

#### 4.10.4.3 IM Exit Message Tables

**Table 4-170 – IM\_Exit\_State\_Change\_Req over R6**

IE	Reference	M/O	Notes
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	ID of the BS from which MS is initiating Idle mode Exit.
Paging Information	5.3.2.119	M	
>Anchor PC ID	5.3.2.12	M	PC ID points to MS's anchor Paging Controller, as obtained from the RNG-REQ message.

**Table 4-171 – IM\_Exit\_State\_Change\_Rsp over R6**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Code value = 32. Included in the event of failure.
BS Info	5.3.2.26	M	
> BS ID	5.3.2.25	M	ID of the BS from which MS is initiating Idle mode Exit.
> AK Context	5.3.2.6	M	AK, AKID, Lifetime, AK Sequence, EIK.
>>AK	5.3.2.5	M	
>>AK ID	5.3.2.7	M	
>>AK Lifetime	5.3.2.8	M	



IE	Reference	M/O	Notes
>>AK SN	5.3.2.9	M	
>>CMAC_KEY_COUNT	5.3.2.34	M	
Paging Information	5.3.2.119	M	
>IDLE Mode Retain Info	5.3.2.81	M	IDLE Mode Retain Info.
MS Info	5.3.2.103	M	
>SBC context	5.3.2.174	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005.
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and DL management connections. If TLV is missing, HARQ is not used on management connections.
>>>HARQ Channel Mapping	5.3.2.455	O	Indicates one or more HARQ channel numbers that may be used for management connections. If TLV is not present then all HARQ channels can be used by management connections.
>>>PDU SN extended subheader for HARQ reordering	5.3.2.456	O	Specifies if PDU SN extended subheader and PDU ordering should be used for management connections. If TLV is not present then PDU SN is not used by management connections
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Supported Security Associations	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>MAC Mode	5.3.2.323	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.

IE	Reference	M/O	Notes
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of UL HARQ Channel	5.3.2.331	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of DL HARQ Channels	5.3.2.334	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Support	5.3.2.336	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator for MIMO Support	5.3.2.343	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
> REG context	5.3.2.144	O	Included based on the bits set in the Idle mode

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

IE	Reference	M/O	Notes
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>Authenticator ID	5.3.2.19	M	Anchor Authenticator of the MS.
>Anchor ASN GW ID	5.3.2.10	M	Anchor DPF/FA of the MS.
>SF Info	5.3.2.185	O	
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and DL management connections. If TLV is missing, HARQ is not used on management connections.
>>>HARQ Channel Mapping	5.3.2.455	O	Indicates one or more HARQ channel numbers that may be used for management connections. If TLV is not present then all HARQ channels can be used by management connections.
>>>PDU SN extended subheader for HARQ reordering	5.3.2.456	O	Specifies if PDU SN extended subheader and PDU ordering should be used for management connections. If TLV is not present then PDU SN is not used by management connections
>>Direction	5.3.2.59	M	
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.
>>ARQ Context	5.3.2.344	O	Contains ARQ related information of the service flow. This context is Mandatory when ARQ enable is set to 1.
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS

IE	Reference	M/O	Notes
			during initial network entry.
>>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>ARQ_SYNC_LOSS_TIME OUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	
>>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule.
>>>> Classification Rule Priority	5.3.2.32	CM	
>>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...
>>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>>> DSCP	5.3.2.409	O	TC bit set to 1
>>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.
>>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV may be included if BE Data Delivery Service is included in the transmitted message.

IE	Reference	M/O	Notes
>>>>Traffic Priority	5.3.2.193	O	This TLV may be included if BE Data Delivery Service is included in the transmitted message.
>>>>Request/Transmission Policy	5.3.2.150	O	This TLV may be included if BE Data Delivery Service is included in the transmitted message.
>>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	This TLV may be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Request/Transmission Policy	5.3.2.150	O	This TLV may be included if UGS Data Delivery Service is included in the transmitted message.
>>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV may be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Traffic Priority	5.3.2.193	O	This TLV may be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Request/Transmission Policy	5.3.2.150	O	This TLV may be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted

IE	Reference	M/O	Notes
			message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV may be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Traffic Priority	5.3.2.193	O	This TLV may be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Request/Transmission Policy	5.3.2.150	O	This TLV may be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV may be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Traffic Priority	5.3.2.193	O	This TLV may be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Request/Transmission Policy	5.3.2.150	O	This TLV may be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>>Media Flow Type	5.3.2.94	O	
>>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>>Reduced Resources Code	5.3.2.237	O	

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



IE	Reference	M/O	Notes
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.

1 **Table 4-172 – Path\_Reg\_Ack over R6**

IE	Description	M/O	Notes
Failure Indication	5.3.2.69	O	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS. performing operation. Included during IM Mode Exit procedure.
> Serving/Target Indicator	5.3.2.182	M	Set to “Serving”.

2 **Table 4-173 – IM\_Exit\_State\_Change\_Req over R4**

IE	Reference	M/O	Notes
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	ID of the BS from which MS is initiating Idle mode Exit.
Paging Information	5.3.2.119	M	
> Anchor PC ID	5.3.2.12	M	PC ID points to MS’s anchor Paging Controller, as obtained from the RNG-REQ.

3 **Table 4-174 – IM\_Exit\_State\_Change\_Rsp over R4**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Code value = 32. Included in the event of failure.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	ID of the BS from which MS is initiating Idle mode Exit.
>AK Context	5.3.2.6	M	AK, AKID, Lifetime, AK Sequence, EIK.
>>AK	5.3.2.5	M	
>>AK ID	5.3.2.7	M	
>>AK Lifetime	5.3.2.8	M	
>>AK SN	5.3.2.9	M	

IE	Reference	M/O	Notes
>>CMAC_KEY_COUNT	5.3.2.34	M	
MS Info	5.3.2.103	M	
>SBC Context	5.3.2.174	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005.
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Supported Security Associations	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>MAC Mode	5.3.2.323	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of UL HARQ Channel	5.3.2.331	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of DL HARQ Channels	5.3.2.334	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Support	5.3.2.336	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator for MIMO Support	5.3.2.343	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>REG context	5.3.2.144	O	Included based on the bits set in the Idle mode retain information TLV. See IEEE802.16e-2005.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per	5.3.2.296	CM	This TLV SHALL be included if REG Context is

IE	Reference	M/O	Notes
Frame Support			included in the transmitted message.
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>Authenticator ID	5.3.2.19	M	Anchor Authenticator of the MS.
>SF Info	5.3.2.185	O	
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.
>>Direction	5.3.2.59	M	
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.
>>ARQ Context	5.3.2.344	O	Contains ARQ related information of the service flow. This context is Mandatory when ARQ enable is set to 1.
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_SYNC_LOSS_TIME OUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	
>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule.
>>>Classification Rule Priority	5.3.2.32	CM	
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.

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

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

IE	Reference	M/O	Notes
>>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>>Reduced Resources Code	5.3.2.237	O	
>>>PHS Rule	5.3.2.127	O	
>>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHS Rule Action	5.3.2.128	CM	Mandatory if PHS-Rules are present.
> Anchor ASN GW ID	5.3.2.10	M	Anchor DPF/FA of the MS.
> SA Descriptor (one or more)	5.3.2.170	O	Included in this message by the BS (if cached a priori by that BS) and is in response to bits set in the Idle mode retain information TLV received from the MS.
>>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.
>>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>>RxPN Counter	0	O	When AES CCM is selected, the TLV SHALL be included.
>>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be



IE	Reference	M/O	Notes
			included.
>>>RxPN Counter	0	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
Paging Information	5.3.2.119	M	
>IDLE Mode Retain Info	5.3.2.81	M	IDLE Mode Retain Info.
Refresh IP address trigger	5.3.2.375	O	Included for the BS to trigger IP address refresh on the MS via HO Process Optimization TLV Bit #13. Currently used only for Simple IP re-anchoring.

**Table 4-175 – IM\_Exit\_State\_Ind**

IE	Description	M/O	Notes
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation.
MS Info	5.3.2.103	M	
> CMAC_Key_Count	5.3.2.34	M	
> Authenticator ID	5.3.2.19	M	
Idle Mode Exit Indicator	5.3.2.369	M	The values are: <ul style="list-style-type: none"> <li>0 = Idle Mode Exit.</li> <li>1 = MS in Idle Mode.</li> </ul>

**Table 4-176 – IM\_Exit\_State\_Ind\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

**Table 4-177 – Path\_Reg\_Ack over R4**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation.
> Serving/Target Indicator	5.3.2.182	M	Set to “Serving”.

**Table 4-178 – Context Req over R4**

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Bitmap indicating the required context. Set to indicate the AK Context.
BS Info (Serving)	5.3.2.26	M	
> BS ID	5.3.2.25	M	The BSID received in the R4 IM_Exit_State_Change_Req.

**Table 4-179 – Context Rpt over R4**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Provide failure indication for this message.
Context Purpose Indicator	5.3.2.36	M	
BS Info (Serving)	5.3.2.26	M	
> BS ID	5.3.2.25	M	BSID received in the corresponding R4 Context Request.
> AK Context	5.3.2.6	M	
>>AK	5.3.2.5	M	
>>AK ID	5.3.2.7	M	
>>AK Lifetime	5.3.2.8	M	
>>AK SN	5.3.2.9	M	
>>CMAC_KEY_COUNT	5.3.2.34	M	

#### 4.10.5 Idle Mode Entry

Both MS and the network may initiate the procedure of entering Idle Mode.

#### 4.10.5.1 MS Initiated Idle Mode Entry

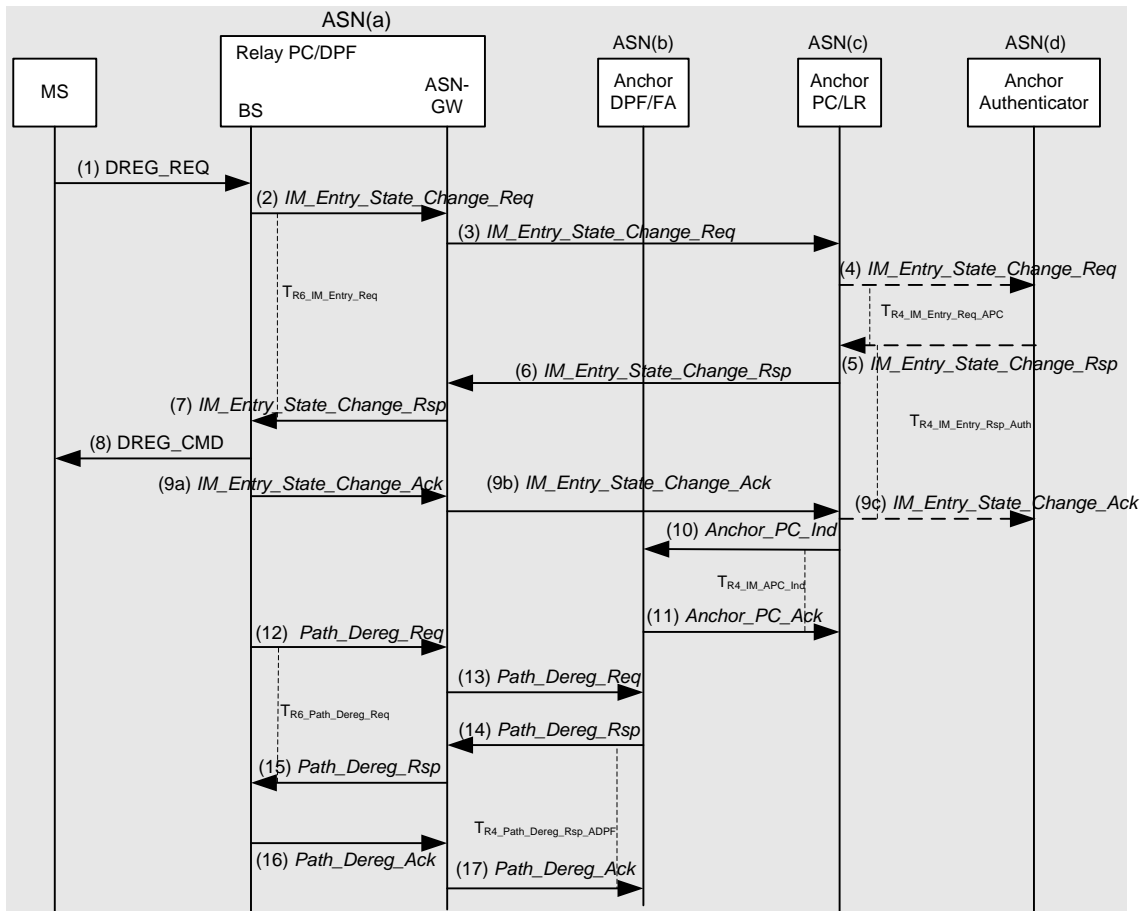


Figure 4-161 – MS Initiated Idle Mode Entry

##### STEP 1

MS decides to enter Idle Mode and sends DREG\_REQ formatted as described in IEEE 802.16e. The De-Registration Request code is set to 0x01 indicating that the MS intends to enter Idle Mode.

##### STEP 2

Based on the MS's request, the BS(PA) in ASN(a) sends an R6 *IM\_Entry\_State\_Change\_Req* message to its ASN-GW. Timer  $T_{R6\_IM\_Entry\_Req}$  is started to monitor R6 *IM\_Entry\_State\_Change\_Rsp* at the BS(PA).

##### STEP 3

The local Relay PC in ASN(a) chooses an Anchor PC for the MS and sends inter-ASN R4 *IM\_Entry\_State\_Change\_Req* message to the ASN(c) associated with the chosen Anchor PC.

##### 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.

ASN(d) sends an Interim Update with optional UDR to AAA (if Idle-Mode-Notification is turned on).

#### 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, and Idle\_Mode\_Timeout value in Paging Information TLV. If Anchor Authenticator rejects the Idle mode entry request, the Failure Indication TLV will contain the rejection code. Timer  $T_{R4\_IN\_Entry\_Rsp\_Auth}$  is started to monitor R4 *IM\_Entry\_State\_Change\_Ack* at the Anchor Authenticator.

When R4 *IM\_Entry\_State\_Change\_Rsp* for MS entering Idle Mode is sent 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).

#### STEP 7

ASN(a) forwards the R6 *IM\_Entry\_State\_Change\_Rsp* to serving BS(PA) including 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 Idle mode 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.

9c: ASN(c) associated with Anchor PC/LR forward the R4 *IM\_Entry\_State\_Change\_Ack* to the ASN(d), which includes the Anchor Authenticator. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN. Upon reception of this message at Anchor PC, timer  $T_{R4\_IM\_Entry\_Rsp\_Auth}$  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 sent 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 response.

**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.

**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).

**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.

**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).

**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  $T_{Path\_Dereg\_Rsp\_ADPF}$ .

#### 4.10.5.2 Network Initiated Idle Mode Entry

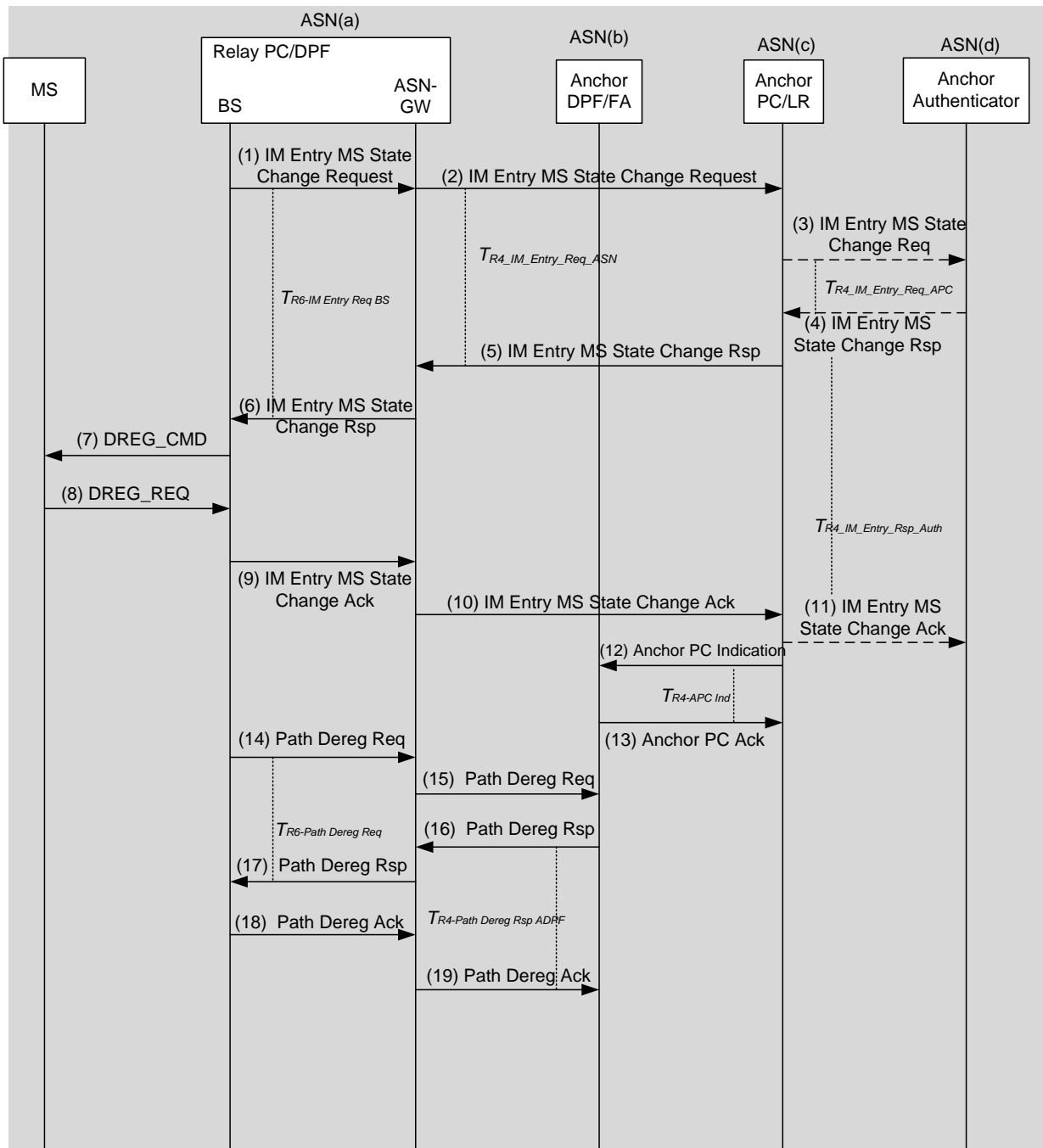


Figure 4-162 – Network Initiated Idle Mode Entry

Network may also initiate the MS Idle Mode Entry procedure. Network initiated Idle Mode entry is triggered by 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 recommend 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 to monitor the R4 *IM\_Entry\_MS\_State\_Change\_Rsp* from the Anchor PC.

**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 send 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, and Idle\_Mode\_Timeout value in Paging Information TLV. If Idle mode entry is not allowed, the Failure Indication 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. Timer  $T_{R4\_IN\_Entry\_Rsp\_Auth}$  is started to monitor R4 *IM\_Entry\_State\_Change\_Ack* at the Anchor Authenticator.

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.

**STEP 6**

Relay PC in ASN(a) forwards the message as R6 *IM\_Entry\_State\_Change\_Rsp* message to related Serving BS(PA). 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 with Action Code TLV set to 0x05 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. The REQ-duration TLV may be included to indicate to the MS when to go to into Idle Mode. If the REQ-duration TLV is not included in the message, the Serving BS sets Timer  $T_{46}$ .

**STEP 8**

MS sends DREG-REQ to the BS(PA) as specified in IEEE 802.16e., acknowledging the Idle mode entry. . If the *REQ-duration* TLV was not sent to the MS, the MS responds with DREG-REQ with message with *De-Registration\_Request\_Code* TLV set to 0x02 prior to expiration of the  $T_{46}$  timer. If the *REQ-duration* TLV was sent to the MS, the MS responds with the DREG-REQ message after expiration of the *REQ-duration* timer with *De-Registration\_Request\_Code* TLV set to 0x01, and the serving BS sends a new DREG-CMD message with Action Code TLV set to 0x05.

**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.)

**STEP 10**

The Relay PC in ASN(a) forwards the message as R4 *IM\_Entry\_State\_Change\_Ack* to the Anchor PC in ASN(c) to indicate that the MS has successfully entered Idle mode and update the status. Upon reception of this message at ASN(c) timer  $T_{R4\_IM\_Entry\_Rsp\_APC}$  is stopped.

If MS has successfully entered Idle mode, ASN(d) sends an Interim Update with optional UDR to AAA (if Idle-Mode-Notification is turned on).

**STEP 11**

ASN(c) associated with Anchor PC/LR forward the R4 *IM\_Entry\_State\_Change\_Ack* to the ASN(d), which includes the Anchor Authenticator. This step is optional if the Anchor Authenticator and Anchor PC/LR are collocated in the same ASN. Upon reception of this message at Anchor authenticator, timer  $T_{R4\_IM\_Entry\_Rsp\_Auth}$  is stopped.

**STEP 12**

The ASN(c) associated with Anchor PC/LR sends the anchor PC indication to Anchor DPF/FA and informs the DPF/FA of MS entering the idle mode. ASN(c) starts timer  $T_{R4\_APC\_Ind}$  at the sending of this message.

**STEP 13**

The ASN(b) associated with Anchor DPF/FA finally updates the information of MS including the Anchor PC ID of this MS and SHALL confirm the procedure by sending R4 *Anchor\_PC\_Ack* to the ASN(c). ASN(c) stops timer  $T_{R4\_APC\_Ind}$  at the receipt of this Anchor PC Ack.

**STEP 14**

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-GW in serving ASN(a). After sending *Path\_Dereg\_Req* to the ASN(a) the BS starts timer  $T_{R6\_Path\_Dereg\_Req}$  to monitor the response.

**STEP 15**

ASN-GW in ASN(a) forwards the message as R4 Path Dereg Req to the ASN(b) associated with the Anchor DPF/FA.

**STEP 16**

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) forwards the message to the BS as R6 Path Dereg Response. Upon reception of this message  $T_{R6\_Path\_Dereg\_Req}$  is stopped.

**STEP 17**

The BS completes the Data Path Dereg process for this MS and acknowledges it by sending R6 *Path\_Dereg\_Ack* to the ASN-GW in ASN(a).

**STEP 18**

ASN-GW in 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  $T_{R4\_Path\_Dereg\_Rsp\_ADPF}$ .

**4.10.5.3 Idle Mode Entry Timers and Timing Considerations:**

This section defines the timer entities defined for the Idle Mode entry procedure.

- $T_{R6\_IM\_Entry\_Req}$ : Started by the Serving BS when it sends R6 *IM\_Entry\_State\_Change\_Req* message to its ASN-GW. This timer is stopped when ASN-GW response R6 *IM\_Entry\_State\_Change\_Rsp* is received.



- $T_{R4\_IM\_Entry\_Req\_ASN}$ : Started by the Serving ASN when it sends  $R4\_IM\_Entry\_State\_Change\_Req$  message. This timer is stopped when ASN-GW response  $R4\_IM\_Entry\_State\_Change\_Rsp$  is received.
- $T_{R4\_IM\_Entry\_Req\_APC}$ : Started by the Anchor PC/LR when it sends  $R4\_IM\_Entry\_State\_Change\_Req$  message to the Authenticator. This timer is stopped when Authenticator responds with  $R4\_IM\_Entry\_State\_Change\_Rsp$ .
- $T_{R4\_IM\_Entry\_Rsp\_Auth}$ : Started by the Anchor Authenticator when it sends  $R4\_IM\_Entry\_State\_Change\_Rsp$ . This timer is stopped when  $R4\_IM\_Entry\_State\_Change\_Ack$  is received.
- $T_{R4\_APC\_Ind}$ : Started by the Anchor PC/LR when it sends  $R4\_Anchor\_PC\_Ind$  to the Anchor DPF/FA. This timer stopped when Anchor PC Ack is received.
- $T_{R6\_Path\_Dreg\_Req}$ : Started by the Serving BS when it sends  $R6\_Path\_Dereg\_Req$  message to the ASN-GW in serving ASN(a). This timer is stopped when serving ASN-GW response  $R6\_Path\_Dereg\_Rsp$  is received.
- $T_{R4\_Path\_Dreg\_Rsp\_ADPF}$ : Started by the ADPF when it sends  $R4\_Path\_Dereg\_Rsp$  message to the serving ASN. This timer is stopped when serving ASN response  $R4\_Path\_Dereg\_Ack$  is received.
- $T_{46}$ : is started by the serving BS after sending a DREG-CMD message to the MS for network initiated Idle Mode. The  $T_{46}$  timer is not set if the MS is instructed to enter Idle Mode at a later time.

Table 4-180 shows the default value of timers and also indicates the range of the recommended duration of these timers.

**Table 4-180 – Idle Mode Entry Timer Values**

Timer	Default Values (msec)	Criteria	Maximum Value
$T_{R6\_IM\_Entry\_Req}$	TBD		TBD
$T_{R4\_IM\_Entry\_Req\_APC}$	TBD		TBD
$T_{R4\_APC\_Ind}$	TBD		TBD
$T_{R6\_Path\_Dreg\_Req}$	TBD		TBD
$T_{R4\_Path\_Dreg\_Rsp\_ADPF}$	TBD		TBD
$T_{46}$	TBD		TBD
$T_{R4\_IM\_Entry\_Req\_ASN}$	TBD		TBD
$T_{R4\_IM\_Entry\_Rsp\_Auth}$	TBD		TBD

#### 4.10.5.4 Idle Mode Entry Error Conditions

This section describes error conditions associated with the Idle Mode entry procedure.

#### 4.10.5.5 Timer Max Retries

Table 4-181 shows details on 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 4-181.

**Table 4-181 – 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

Timer	Entity where Timer Started	Action(s)
		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 <sub>R4_IM_Entry_Req_APC</sub>	Anchor PC	No Action Required.
T <sub>R4_APC_Ind</sub>	Anchor PC	Sends R4 <i>IM_Entry_State_Change_Req</i> 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 <sub>R4_IM_Entry_Rsp_Auth</sub>		Failure indication sent downstream to the Anchor PC/LR.
T <sub>R6_Path_Dreg_Req</sub>		The BS will perform error handling as per local policy.
T <sub>R4_Path_Dreg_Rsp_ADPF</sub>		The Anchor DPF will perform error handling as per local policy.
T <sub>R4_IM_Entry_Req_ASN</sub>	Serving ASN	No Action Required.
T <sub>46</sub>	BS	BS stops sending DREG-CMD to MS. Network initiated Idle Mode entry fails.

#### 4.10.5.6 AK Context Generation Error

Upon receiving the R4 *IM\_Entry\_State\_Change\_Req* message the Anchor Authenticator verifies the MS is allowed to go idle and it is possible for network to support the MS in Idle mode. If Authenticator makes a decision it is possible and allowed to go idle mode, R4 *IM\_Entry\_State\_Change\_Rsp* is given to Anchor PC. 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, it 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 serving BS and ASN-GW which may drop the Idle mode entry procedures.

#### 4.10.5.7 R6 Data Path Deregistration Error

This error refers to the inability of deregistering 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 Dereg Response message back to the serving BS. The serving BS upon receipt of the message, takes appropriate failure recovery action on the R6 data path which are beyond the scope of this specification.

#### 4.10.5.8 R4 Data Path Deregistration Error

This error refers to the inability of deregistering 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 Dereg Response message back to the serving ASN. The serving ASN upon receipt of the message, takes appropriate failure recovery action on the R4 data path which are beyond the scope of this specification.

#### 4.10.5.9 IM Entry Message Tables

**Table 4-182 – IM\_Entry\_State\_Change\_Req over R6**

IE	Reference	M/O	Notes
BS Info	5.3.2.26	M	
> BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation.
MS Info	5.3.2.103	M	
>SBC Context	5.3.2.174	O	Included based on the bits set in the Idle mode retain information TLV from the MS or if cached by the BS.
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and DL management connections. If TLV is missing, HARQ is not used on management connections.
>>>HARQ Channel Mapping	5.3.2.455	O	Indicates one or more HARQ channel numbers that may be used for management connections. If TLV is not present then all HARQ channels can be used by management connections.
>>>PDU SN extended subheader for HARQ reordering	5.3.2.456	O	Specifies if PDU SN extended subheader and PDU ordering should be used for management connections. If TLV is not present then PDU SN is not used by management connections.
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Supported Security Associations	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>MAC Mode	5.3.2.323	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security

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

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

IE	Reference	M/O	Notes
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
> SA Descriptor (one or more)	5.3.2.170	O	Included based on the bits set in the Idle mode retain information TLV from the MS or if cached by the BS.
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	0	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be

IE	Reference	M/O	Notes
			included.
>>>RxPN Counter	0	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>SF Info	5.3.2.185	M	Service Flow Information of the MS. Contains Service Flow information in the nested IEs.
>>SFID	5.3.2.184	M	
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and DL management connections. If TLV is missing, HARQ is not used on management connections.
>>>HARQ Channel Mapping	5.3.2.455	O	Indicates one or more HARQ channel numbers that may be used for management connections. If TLV is not present then all HARQ channels can be used by management connections.
>>>PDU SN extended subheader for HARQ reordering	5.3.2.456	O	Specifies if PDU SN extended subheader and PDU ordering should be used for management connections. If TLV is not present then PDU SN is not used by management connections.
>>Direction	5.3.2.59	M	
>> ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.
>>ARQ Context	5.3.2.344	O	Contains ARQ related information of the service flow. This context is Mandatory when ARQ enable is set to 1.
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_SYNC_LOSS_TIME	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is

IE	Reference	M/O	Notes
OUT			included in the transmitted message.
>>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>CID	5.3.2.29	O	
>>SAID	5.3.2.169	O	
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	
>>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule.
>>>> Classification Rule Priority	5.3.2.32	CM	
>>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.
>>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...
>>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.
>>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.
>>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.
>>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.
>>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.
>>QoS Parameters	5.3.2.141	M	
>>>> DSCP	5.3.2.409	O	TC bit set to 1
>>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.
>>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV may be included if BE Data Delivery Service is included in the transmitted message.
>>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.
>>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted



IE	Reference	M/O	Notes
			message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.

IE	Reference	M/O	Notes
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>Media Flow Type	5.3.2.94	O	
>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>Reduced Resources Code	5.3.2.237	O	
>>PHS Rule	5.3.2.127	O	
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHS Rule Action	5.3.2.128	CM	Mandatory if PHS-Rules are present.
> Authenticator ID	5.3.2.19	M	ID of Anchor Authenticator.
> Anchor ASN GW ID	5.3.2.10	M	ID of Anchor GW / Anchor DPF.
>Mobility Access Classifier	5.3.2.423	O	Shall be included by the BS if the MS mobility access classifier is fixed or nomadic and the BS supports Mobility Restriction for stationary access.
>Reattachment-Zone	5.3.2.424	O	Shall be included by the BS if the MS mobility

IE	Reference	M/O	Notes
			access classifier is included.
Paging Information	5.3.2.119	M	Included based on the Paging Cycle TLV received from MS or if cached by the BS(PA). If not cached in the BS(PA), the BS(PA) will set the Page Group ID part of the TLV and may include the suggested values for Paging cycle and Offset.
> Paging Cycle	5.3.2.118	O	Included based on the Paging Cycle Request TLV received from MS or if cached by the BS.
> Paging Offset	5.3.2.120	O	
> Paging Interval Length	5.3.2.135	O	
> Paging Group ID	5.3.2.123	O	
> Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS, to be stored in Location Register.
> Idle Mode Retain Info	5.3.2.81	O	Included based on the bits set in the Idle mode retain information TLV from the MS or if cached by the BS.

1

2

**Table 4-183 –Anchor\_PC\_Ind**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Included if idle mode entry is not successful.
Paging Information	5.3.2.119	M	Included if Failure Indication is not included.
>Anchor PC ID	5.3.2.12	M	Confirmed Paging Controller ID for the MS entering Idle mode.

3

**Table 4-184 –Anchor\_PC\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

4

**Table 4-185 – IM\_Entry\_State\_Change\_Req over R4**

IE	Reference	M/O	Notes
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation.
MS Info	5.3.2.103	M	
>SBC Context	5.3.2.174	O	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005. Optionally included in this R4 message if present in the corresponding R6

IE	Reference	M/O	Notes
			message.
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Supported Security Associations	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>MAC Mode	5.3.2.323	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of UL HARQ Channel	5.3.2.331	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>The number of DL HARQ Channels	5.3.2.334	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Support	5.3.2.336	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA SS modulator for MIMO Support	5.3.2.343	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.
>REG context	5.3.2.144	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.
>>Number of UL Transport CIDs Support	5.3.2.288	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Number of DL Transport CIDs Support	5.3.2.289	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per Frame Support	5.3.2.296	CM	This TLV SHALL be included if REG Context is included in the transmitted message.

IE	Reference	M/O	Notes
>>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support is included in the transmitted message.
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO Connections Parameters Proc Time	5.3.2.308	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>MAC Header and Extended Sub-Header Support	5.3.2.310	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>System Resource Retain Timer	5.3.2.311	O	
>>MS Handover Retransmission Timer	5.3.2.312	O	
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.
>Authenticator ID	5.3.2.19	M	

IE	Reference	M/O	Notes
>Mobility Access Classifier	5.3.2.423	O	Shall be included if the MS mobility access classifier is fixed or nomadic and the serving BS supports Mobility Restriction for stationary access.
>Reattachment-Zone	5.3.2.424	O	Shall be included if the MS mobility access classifier is included.
>SA Descriptor (one or more)	5.3.2.170	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.
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	0	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.
>>>RxPN Counter	0	O	When AES CCM is selected, the TLV SHALL be included.
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.

IE	Reference	M/O	Notes
>SF Info	5.3.2.185	M	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005. Contains Service Flow information in the nested IEs.
>> SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.
>> ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.
>>ARQ Context	5.3.2.344	O	Contains ARQ related information of the service flow. This context is Mandatory when ARQ enable is set to 1.
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_SYNC_LOSS_TIME OUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_RX_PURGE_TIMEO UT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>>RECEIVER_ARQ_ACK_P ROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.
>>Direction	5.3.2.59	M	
>>SAID	5.3.2.169	O	
>>QoS Parameters	5.3.2.141	M	
>>> DSCP	5.3.2.409	O	TC bit set to 1
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	This TLV may be included if BE Data Delivery Service is included in the transmitted message.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.



IE	Reference	M/O	Notes
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Polling Interval	5.3.2.200	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission	5.3.2.150	O	See IEEE802.16e for further details.

IE	Reference	M/O	Notes
Policy			
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Unsolicited Grant Interval	5.3.2.199	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.
>>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.
>>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.
>>>>Media Flow Type	5.3.2.94	O	
>>>>Media Flow Description in SDP Format	5.3.2.228	O	
>>>>Reduced Resources Code	5.3.2.237	O	
>>PHS Rule	5.3.2.127	O	
>>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSF	5.3.2.124	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>>PHS Rule Action	5.3.2.128	CM	Mandatory if PHS-Rules are present.
Paging Information	5.3.2.119	M	Paging Information TLV obtained from the BS containing PAGING_CYCLE, PAGING_OFFSET,

IE	Reference	M/O	Notes
			and Paging Group ID if present in R6 message.
> Paging Cycle	5.3.2.118	O	
> Paging Offset	5.3.2.120	O	
> Paging Interval Length	5.3.2.135	O	
> Paging Group ID	5.3.2.123	O	
> Idle Mode Retain Info	5.3.2.81	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.
>Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS, to be stored in Location Register.
>Anchor PC ID	5.3.2.12	M	Recommended Anchor PC ID by the Relay PC.
>Anchor ASN GW ID	5.3.2.10	M	ASN GW associated with Anchor DPF/FA. This MUST be same as that received on R6.

1

**Table 4-186 – IM\_Entry\_State\_Change\_Rsp**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Optional TLV if there is a failure.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation. (To indicate destination BS for a relayed message, this IE is needed).
Paging Information	5.3.2.119	M	Paging Information TLV meant for the DREG-CMD to the MS containing PAGING_CYCLE, PAGING_OFFSET, PAGING_INTERVAL_LENGTH and Paging Group ID Confirmed and stored by the Anchor PC.  When this message is sent from Authenticator to Anchor-PC, this TLV SHALL include Idle_Mode_Timeout.
>Anchor PC ID	5.3.2.12	O	Included if Paging Controller ID different than the APC received in R4 <i>IM_Entry_State_Change_Req</i> message.
> Paging Cycle	5.3.2.118	O	Included if different than that received in R4 <i>IM_Entry_State_Change_Req</i> .
> Paging Offset	5.3.2.120	O	Included if different than that received in R4 <i>IM_Entry_State_Change_Req</i> .
> Paging Interval Length	5.3.2.135	O	Included if different than that received in R4 <i>IM_Entry_State_Change_Req</i> .

IE	Reference	M/O	Notes
> Paging Group ID	5.3.2.123	O	This TLV SHALL be included if Paging Information is included in the transmitted message.
> Idle Mode Retain Info	5.3.2.81	O	The Anchor PC/LR SHALL include this if does not accept the settings of the Idle Mode Retain Info received in the R6 <i>IM_Entry_State_Change_Req</i> .
> Idle Mode Timeout	5.3.2.268	M	The Anchor PC/LR SHALL include to minimize Timeout mismatch between the system and devices.
MS Info	5.3.2.103	M	
>Mobility Access Classifier	5.3.2.423	O	Included by the Authenticator to the Anchor PC if the MS mobility access classifier is fixed or nomadic.
>Reattachment-Zone	5.3.2.424	O	Included by the Authenticator to the Anchor PC if the MS mobility access classifier is fixed or nomadic.

**Table 4-187 – IM\_Entry\_State\_Change\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	Optional TLV if there is a failure by rejection of MS. Code Value = 52
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS performing operation.
Paging Information	5.3.2.119	M	
>Anchor PC ID	5.3.2.12	M	Paging Controller ID Acting as Anchor PC.

#### 4.10.6 Idle Mode Operation and CSN Anchored Mobility Management

Support for Foreign Agent migration in Idle Mode is optional. FA migration is supported only for CMIP and PMIP. Support for each of the distinct, different methods of FA migration in Idle Mode is optional.

If FA migration in Idle Mode is supported, FA migration in Idle Mode SHALL only occur at an indeterminate, implementation specific time after any successful Secure Location Update.

If FA migration in Idle Mode is supported, the network SHALL be aware of the MS mobility management client type, either CMIP or PMIP, and the network topology, and employ the appropriate FA migration method.

##### 4.10.6.1 Anchor DPF and FA

Anchor DPF and FA are collocated in the event that FA is present (which will be in the case of CMIP4 and PMIP4). In the event that there is no FA present in the network (which will be in the case of Simple IPv4/6, MIP6), the Anchor DPF is an independent functional entity. In the case of IPv6 and MIP6, there will be an anchor DPF functional entity that is instantiated at the AR when the IPv6 ISF is established.

#### 4.10.6.2 CMIP in Idle Mode

The optional migration of Foreign Agent while the MS is in idle mode (e.g., when Idle mode MS moves or for other implementation reasons) requires that MS exit Idle mode and complete network reentry to complete MIP registration procedures [48]. If the MS exits Idle mode to complete MIP registration for FA migration, the network reentry and subsequent Idle mode entry procedures SHALL comply with relevant sections of this document. Figure 4-163 and Figure 4-165 show a FA migration following a successful location update. The FA migration can be initiated by the Anchor PC or the new (target) FA.

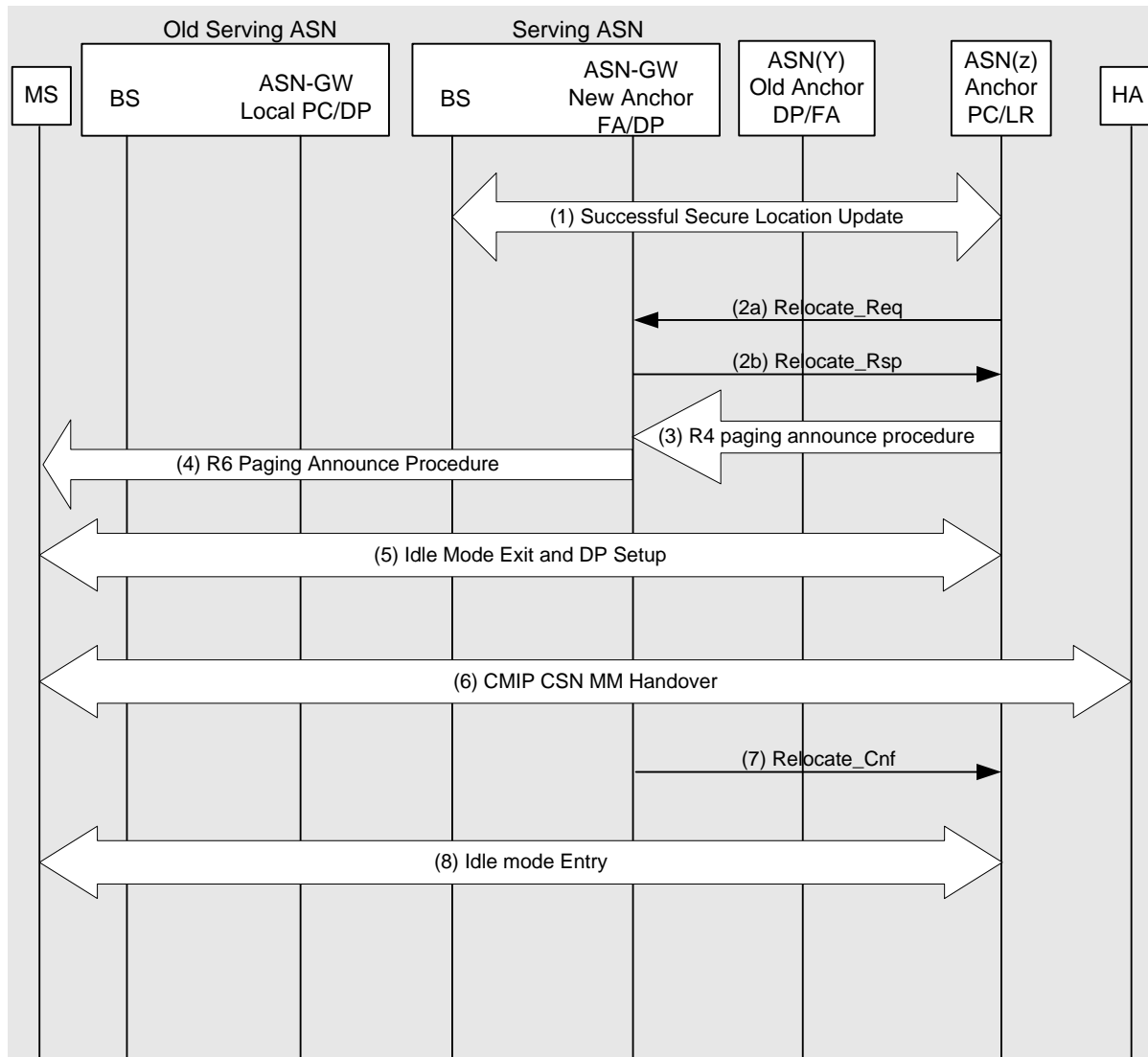
If the FA migration does not occur in Idle mode, data path establishment MAY occur across multiple ASNs when the MS exits Idle mode after moving across ASNs. When the MS exits Idle mode due to incoming or outgoing data to/from the MS, it SHALL perform MIP registration procedures for FA migration and data path optimization across R3 to the HA. The timing for FA migration in this case is implementation and deployment dependent.

##### 4.10.6.2.1 FA Migration During Idle Mode: Anchor PC Initiated

This call flow shows a FA migration following a successful location update. The MS performs a mobility event (i.e., inter-ASN idle mode handoff) such that it moves to a new serving BS/ASN and performs a location update. Upon completion of the Location update procedure the Anchor PC determines that a FA migration is needed and will proceed to initiate paging procedures to exit the MS out of idle mode.

##### 4.10.6.2.1.1 Trigger to New FA

This section defines steps for FA Migration where the Anchor PC sends a trigger to the new FA to initiate the FA Migration procedure.



**Figure 4-163 – FA Migration During Idle Mode: Anchor PC Initiated (Trigger to New FA)**

### STEP 1

The MS performs a secure location update with the Anchor PC (see section 4.10.2 for details on this procedure).

### STEP 2

The Anchor-PC determines that a FA migration is needed. Details on determination of when a FA migration is needed are outside the scope of this document. The Anchor PC/ASN send R4 *Relocation Req* message to the new selected FA. In this call scenario is assumed that the selected FA accepts the re-location request and responds with R4 *Relocation Rsp* message.

### STEP 3

The Anchor-PC initiates R4 paging procedures and send R4 *Paging Announce* message to the Local PC. The Anchor PC includes the new FA ID in the *Paging Announce* message.

**STEP 4**

The Local-PC initiates R6 paging procedures with the MS.

**STEP 5**

The MS performs idle mode exit procedures (as specified in section 4.10.4) and establishes a DP to with the new anchor DPF.

**STEP 6**

This step is performed the same way as defined in section 4.8.3.3.7 CMIP CSN MM Handover.

**STEP 7**

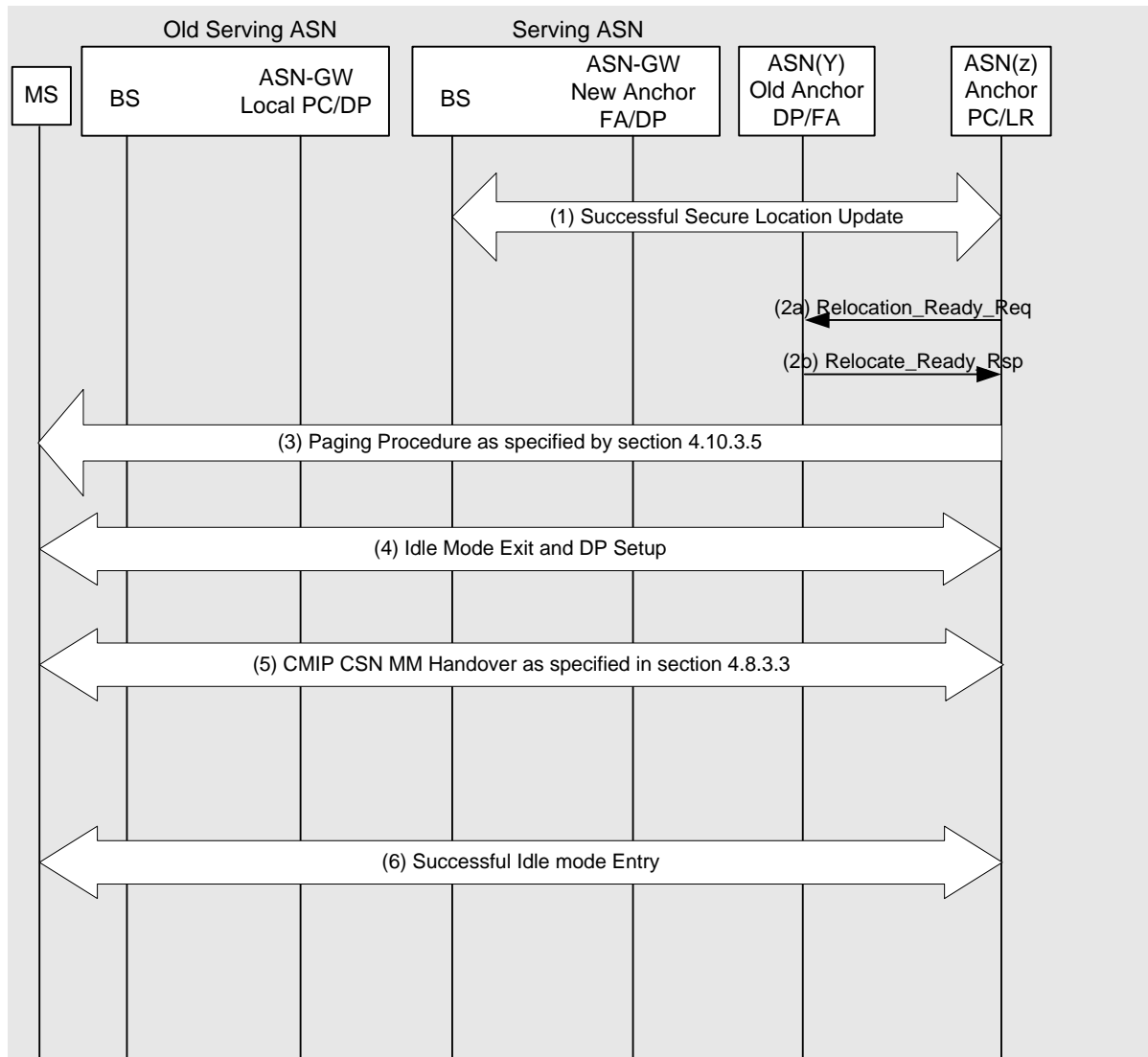
Upon successful registration of the MS with the HA, the FA sends a R4 *Relocation\_Cnf* message to the Anchor PC.

**STEP 8**

The Serving ASN initiates network initiated idle mode entry procedures (as specified in section 4.10.5.2) to transition the MS to the idle mode.

**4.10.6.2.1.2 Trigger to Old FA**

This section defines steps for FA Migration where the Anchor PC sends a trigger to the old FA to initiate the FA Migration procedure.



**Figure 4-164 – FA Migration During Idle Mode: Anchor PC Initiated (Trigger to Old FA)**

**STEP 1**

The MS performs a secure location update with the Anchor PC (see section 4.10.2 for details on this procedure).

**STEP 2**

The Anchor PC/ASN sends *Relocation\_Ready\_Req* message to the old FA. In this call scenario is assumed that the old FA accepts the re-location request and responds with *Relocation\_Ready\_Rsp* message.

**STEP 3**

The *Relocation\_Ready\_Rsp* received by the Anchor PC contains R3 Relocation Action code. If the R3 Relocation Action code is “Initiate Paging”, the Anchor-PC initiates paging procedures as specified by section 4.10.3.5 with paging cause value set to “R3 Re-Anchoring During Idle Mode”.



**STEP 4**

The MS performs idle mode exit procedures (as specified in section 4.10.4) and establishes a DP with the existing anchor DPF.

**STEP 5**

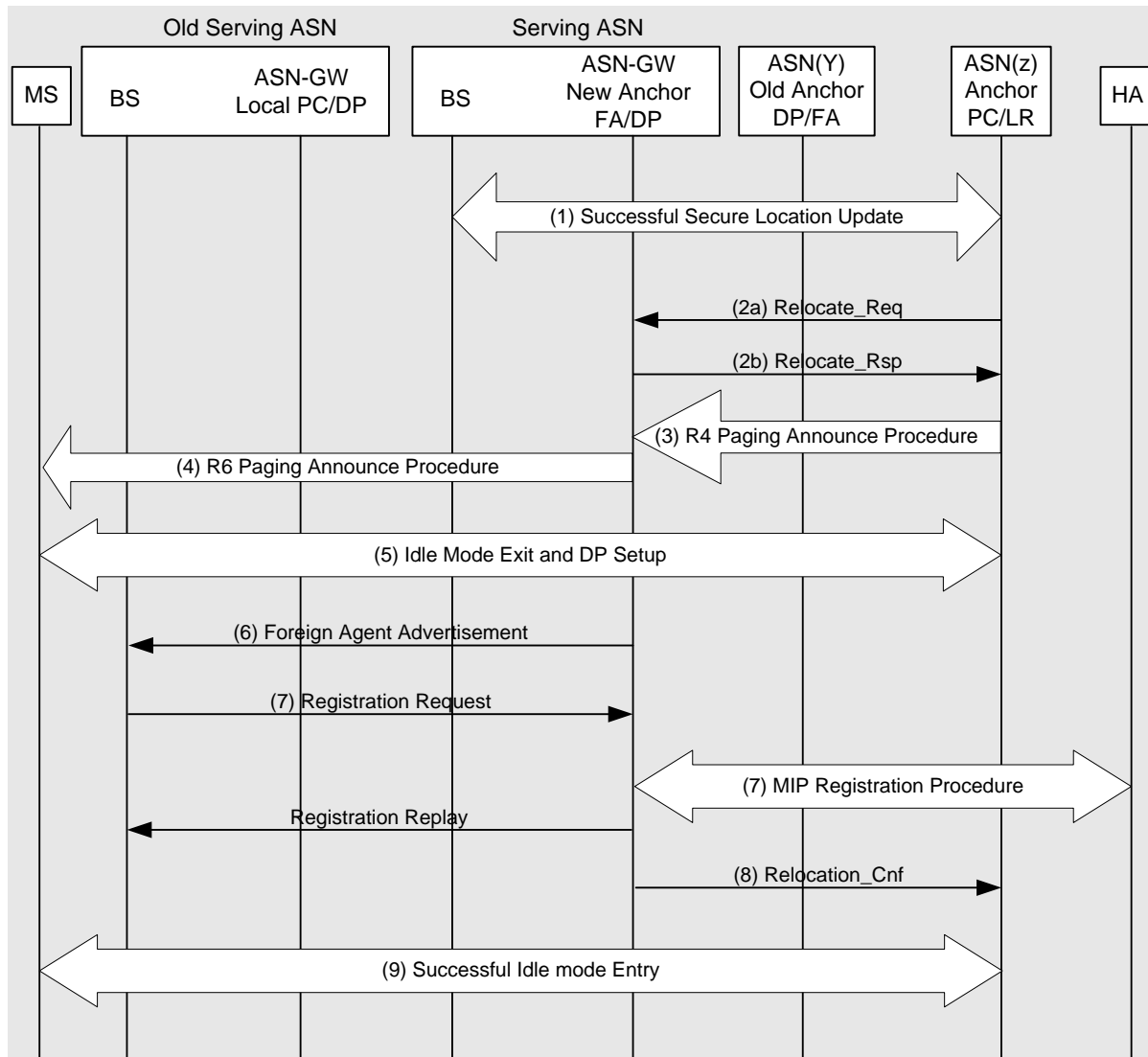
This step is performed the same way as defined in section 4.8.3.3.7 CMIP CSN MM Handover.

**STEP 6**

The Serving ASN initiates network initiated idle mode entry procedures (as specified in section 4.10.5.2) to transition the MS to the idle mode.

**4.10.6.2.2 FA Migration during Idle Mode: New (target) FA Initiated**

This call flow shows a FA migration following a successful location update. The MS performs a mobility event (i.e., inter-ASN idle mode handoff) such that it moves to a new serving BS/ASN and performs a location update. Upon completion of the Location update procedure the new (target) FA determines that a FA migration is needed and will trigger the PC to proceed to initiate paging procedures to exit the MS out of idle mode. Upon successful exit from idle mode, the new FA will send the Foreign Agent Advertisement message to the MS.



**Figure 4-165 – FA Migration During Idle Mode: New (target) FA Initiated**

### STEP 1

The MS performs a secure location update with the Anchor PC (see section 4.10.2 for details on this procedure).

### STEP 2

The New (Anchor) FA determines that a FA migration is needed. Details on determination of when a FA migration is needed are outside the scope of this document. The New (Anchor) FA send R3 *Relocation\_Req* message to the Anchor PC/ASN to trigger paging procedures for the MS. The R3 *Relocation\_Req* message contains the FA ID of the New (Anchor) FA. In this call scenario is assumed that Anchor PC accepts the request to trigger Paging for the MS and responds with R3 *Relocation\_Rsp* message.

### STEP 3

The Anchor-PC initiates R4 paging procedures and send R4 *Paging\_Announce* message to the Local PC. The Anchor PC includes the new FA ID in the *Paging\_Announce* message.

**STEP 4**

The Local-PC initiates R6 paging procedures with the MS.

**STEP 5**

The MS performs idle mode exit procedures (as specified in section 4.10.4) and establishes a DP with the new anchor DPF.

**STEP 6**

Upon completion of the data path, the new FA sends a Foreign Agent Advertisement message to the MS.

**STEP 7**

The MS sends a registration request message to the FA to perform MIP Registration procedures with the HA. The FA sends a registration response message to the MS.

**STEP 8**

Upon successful registration of the MS with the HA, the FA sends a R3 *Relocation\_Cnf* message to the Anchor PC.

**STEP 9**

The Serving ASN initiates network initiated idle mode entry procedures (as specified in section 5.10.5.2) to transition the MS to the idle mode.

**4.10.6.3 PMIP4 in Idle Mode**

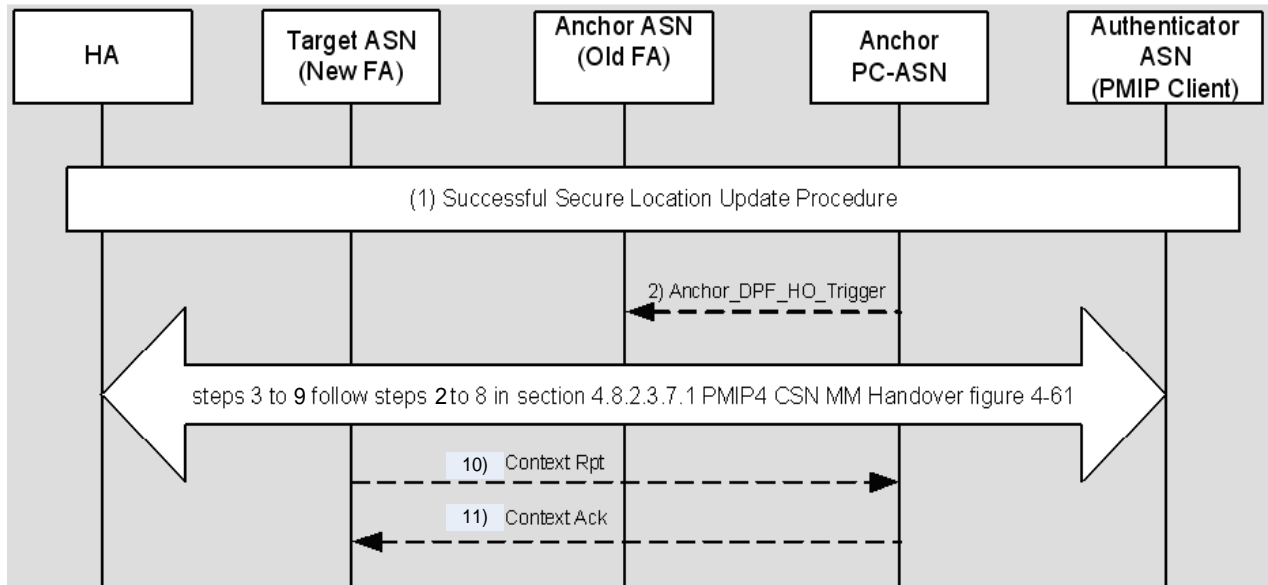
Migration of FA for an Idle mode MS in a PMIP4 enabled ASN MAY be supported. The migration of the FA MAY be triggered when the MS moves across ASNs.

After Secure Location update procedure is complete, either Anchor PC-ASN or Target ASN (New FA) MAY trigger FA migration following the normal CSN MM HO procedure defined in section 4.8.2.3.7.1. The two methods are identified to provide support for topologically aware and topologically unaware network models, but are not limited to such use.

Figure 4-166 illustrates the call flow for FA migration for an Idle Mode MS in a PMIP4 enabled ASN triggered by the Anchor PC-ASN.

Figure 4-167 illustrates the call flow for FA migration triggered by Target ASN (New FA) for an Idle Mode MS in a PMIP4 enabled ASN with Anchor MM context retrieving. The Target ASN (New FA) MAY obtain Anchor MM context information through Context Request and Context Report procedures through Anchor PC-ASN without involving the Secure Location Update procedure.

#### 4.10.6.3.1 PMIP4 in Idle Mode – FA Migration Triggered from the Anchor PC-ASN



**Figure 4-166 – Anchor PC-ASN Triggered FA Migration for an Idle Mode MS in a PMIP-enabled ASN**

##### STEP 1

This depicts a successful Secure Location Update procedure as specified in 4.10.2. An indeterminate, implementation specific time may elapse between Step 1 and Step 2.

##### STEP 2

The Anchor PC ASN sends Anchor\_DPF\_HO\_Trigger to Anchor ASN (ASN) to initiate the FA relocation.

##### STEP 3 - 9

These steps are same as the steps 2 to 8 in section 4.8.2.3.7.1 PMIP4 CSN MM Handover, Figure 4-129.

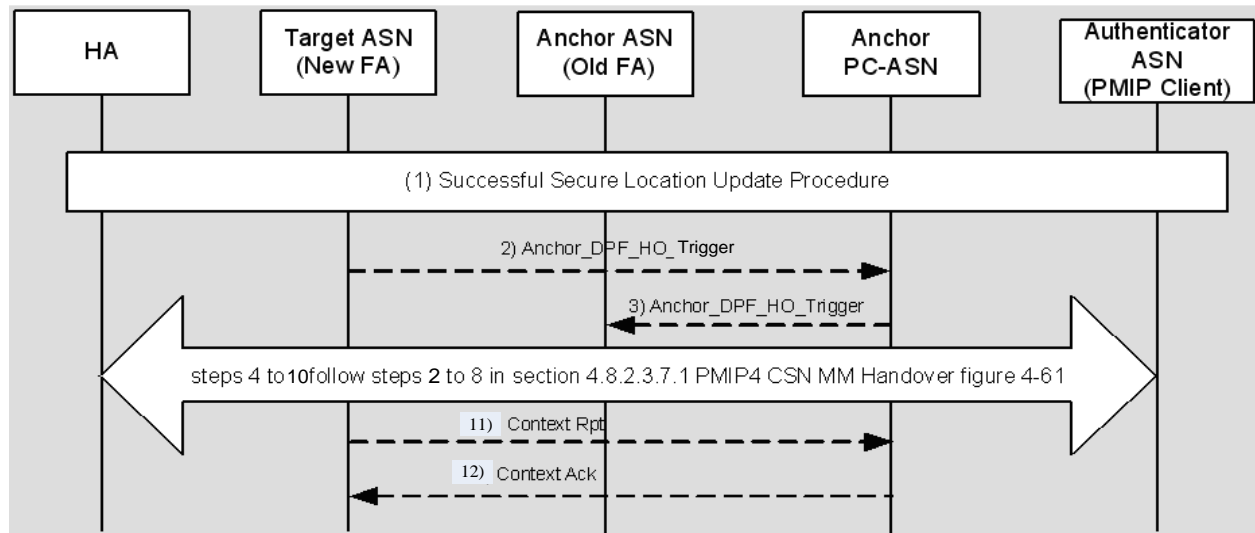
##### STEP 10

If the Target ASN (New FA) and Anchor PC-ASN are not collocated then Target ASN (New FA) updates the Anchor PC-ASN with the Context\_Rpt message, confirming the FA relocation.

##### STEP 11

The Anchor PC-ASN sends Context\_Ack to Anchor ASN (New FA) and updates the MS related context with new FA for the MS.

#### 4.10.6.3.2 PMIP4 in Idle Mode – FA Migration triggered from the Target ASN (New FA)



**Figure 4-167 – Target ASN (New FA) Triggered FA Migration for an Idle Mode MS in a PMIP-enabled ASN**

#### STEP 1

This depicts a successful Secure Location Update procedure as specified in 4.10.2. An indeterminate, implementation specific time may elapse between Step 1 and Step 2.

#### STEP 2

The Target ASN (New FA) sends Anchor\_DPF\_HO\_Trigger to the Anchor PC-ASN to indicate the FA Relocation.

#### STEP 3

If the Anchor PC-ASN agrees with FA relocation, sends Anchor\_DPF\_HO\_Trigger to Anchor ASN (Old FA) to initiate the FA relocation process.

#### STEP 4 - 10

These steps are same as the steps 2 to 8 in section 4.8.2.3.7.1 PMIP4 CSN MM Handover, Figure 4-129.

#### STEP 11

If the Target ASN (New FA) and Anchor PC-ASN are not collocated then Target ASN (New FA) updates the Anchor PC-ASN with the Context\_Rpt message, confirming the FA relocation.

#### STEP 12

The Anchor PC-ASN sends Context\_Ack to Anchor ASN (New FA) and updates the MS related context with New FA for the MS.

#### 4.10.6.4 Idle Mode Operation and Simple IP Re-anchoring

Implementation and use of Simple IP re-anchoring in Idle Mode feature is optional.

In order to optimize the Data Path, Access Router may be migrated from Anchor ASN to Serving ASN during idle mode in Simple IP network. When it is supported, the re-anchoring may be triggered after the location update procedure (regardless of anchor PC relocation).

#### 4.10.6.4.1 Triggering Simple IP Re-anchoring

The successful secure location update may cause triggering of Simple IP Re-anchoring. The network detects the movements of the MS by the location update Procedure. The network decides to re-anchor the Access Router for Simple IP Service to optimize the data path to the network based on the topology information. After successful secure location update procedure, the old authenticator may initiate the Simple IP re-anchoring procedure based on policy and topology information. Note that during the secure location update procedure, the paging controller relocation may be performed.

The MS's idle mode exit procedure may cause triggering of Simple IP Re-anchoring.

#### 4.10.6.4.2 Simple IP Re-anchoring Procedure in Idle mode

When Simple IP Re-anchoring is triggered, the following procedure is performed.

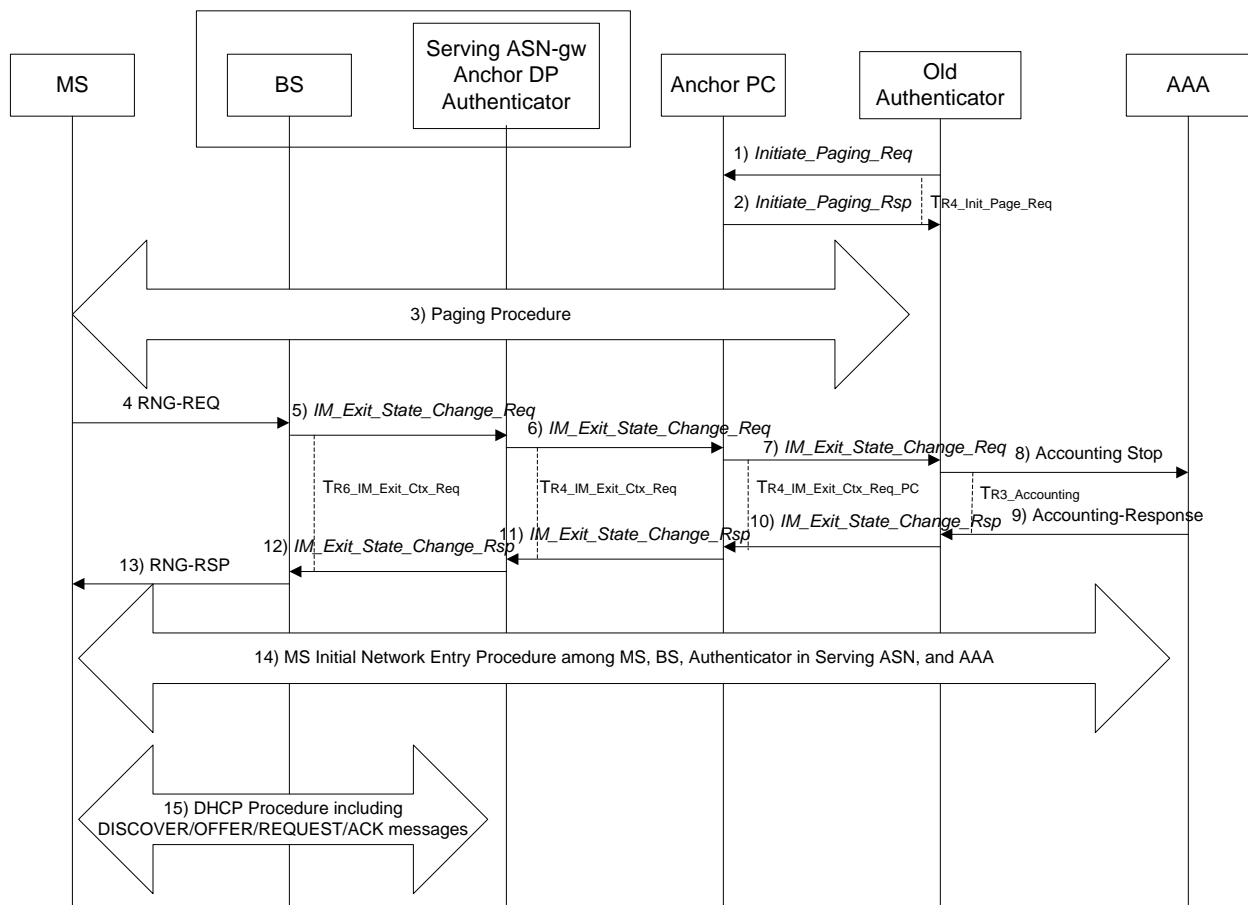


Figure 4-168 – Simple IP Re-anchoring Procedure

#### STEP 1

The anchor authenticator which is described as “Old Authenticator” in the figure initiates Paging Procedure by sending *Initiate\_Paging\_Req* to the Anchor PC. The Old Authenticator starts timer  $T_{Init\_Page\_Req}$ .

#### STEP 2

Anchor PC responds the Old Authenticator with sending an R4 *Initiate\_Paging\_Rsp*. This message is used to indicate whether the MS context as contained in the PC is correct and the requested paging action is authorized.

Exclusion of the Response Code TLV indicates intent to page the MS. Upon receipt of this message the Old Authenticator stops timer TInit\_Page\_Req if running.

### STEP 3

The anchor PC initiates Paging Procedure as described in the section 4.10.3.5 [NWGSTG3]. If the Anchor PC is located in the Serving ASN in case after a successful PC relocation, Paging Procedure is initiated by the Serving ASN.

If this procedure is performed by MS's re-entering the network, the paging procedure doesn't happen.

### STEP 4 ~ STEP 7

Steps 4,5,6 and 7 of this call flow corresponds to the steps 1, 2, 3 and 4 of the Idle Mode Exit Procedure as described in the section 4.10.4.1 [NWGSTG3] – “Idle Mode Exit – Serving ASN Does Not Have MS Context”.

### STEP 8 ~ STEP 9

When the old authenticator decides to perform Simple IP re-anchoring, it performs the RADIUS or Diameter Accounting Stop Procedure. This indicates that the IP session is terminated.

### STEP 10

When the Authenticator decides to perform Simple IP re-anchoring, the old authenticator responds with IM\_Exit\_State\_Change\_Rsp with Refresh IP Address Trigger TLV value set to 1.

Note that Step 10 doesn't have to wait for the completion of step 9.

### STEP 11 ~ STEP 12

Steps 11 and 12 of this call flow corresponds to steps 6 and 7 of Idle Mode Exit procedure as described in this section 4.10.4.1 refer NWG STG3 - – “Idle Mode Exit – Serving ASN Does Not Have MS Context”.

### STEP 13

When the BS receives this message, it sends RNG-RSP with HO Process Optimization TLV in order for MS to perform Full network entry and DHCP procedure according to [13].

Note that BS SHALL set the HO optimization TLV settings to "Full network entry with traffic IP address refresh".

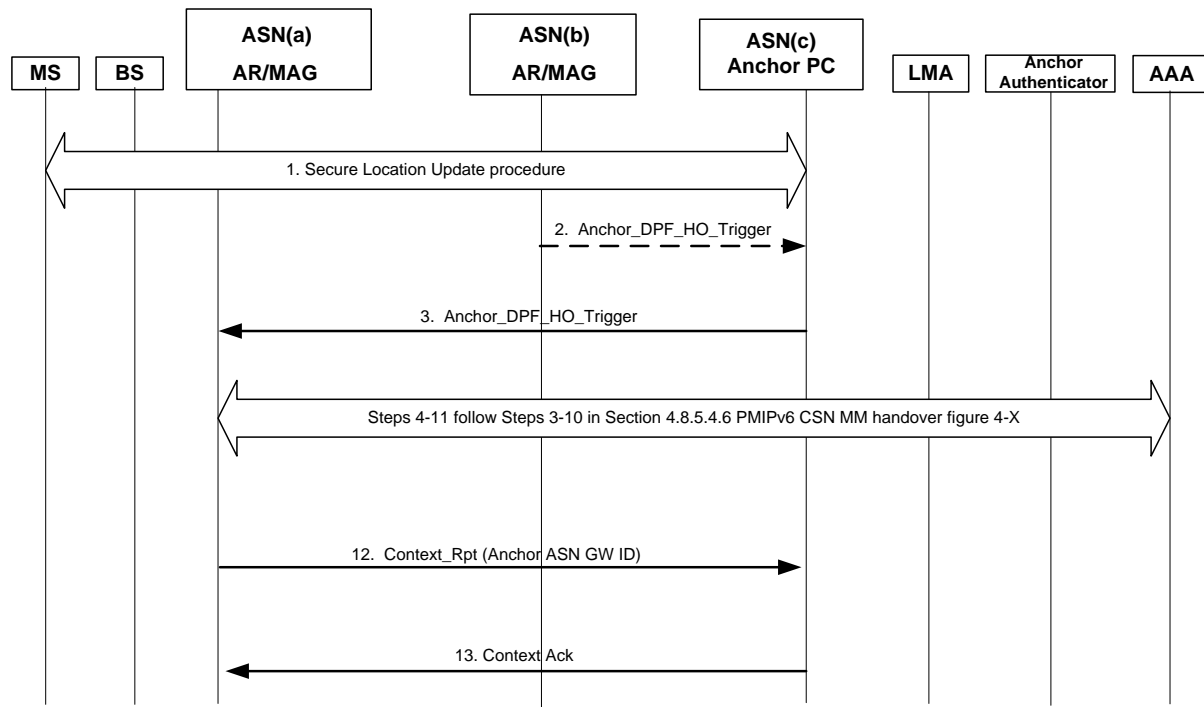
### STEP 14

MS, BS, Authenticator and AAA performs Step 3 to Step 28 of MS initiated Network Entry procedure as described in the section 4.5.1.1 [NWGSTG3]. Network access authentication procedure is required so that the HAAA can deliver the new IP address and be made aware of the IP address change. After successful authentication, the MS and ASN establish Initial Service Flow and appropriate Pre-provisioned Service Flows based on the information from AAA server.

### 4.10.6.5 PMIP6 in Idle Mode

Migration of AR/MAG for an Idle mode MS in a PMIP6 enabled ASN MAY be supported. The migration of the AR/MAG MAY be triggered when the MS moves across ASNs.

Figure 4-169 illustrates the two possible AR/MAG migration scenarios for a MS engaged in a PMIP6 session in the Idle Mode. After Secure Location update procedure is complete the Anchor PC MAY decide to trigger the AR/MAG relocation towards the new PMIP6-enabled target ASN. In the other case the AR/MAG migration MAY be triggered directly by the Target ASN (new AR/MAG) and is in both cases followed by the regular PMIP6 CSN-MM HO procedure as defined in section 4.8.5.5.6 . The Target ASN (new AR/MAG) MAY obtain Anchor MM context information through Context Report procedures from Anchor PC-ASN without involving the Secure Location Update procedure.



**Figure 4-169 – PMIP6 AR/MAG Migration for an Idle Mode MS**

### STEP 1

This depicts a successful Secure Location Update procedure as specified in 4.10.2. An indeterminate, implementation specific time may elapse between Step 1 and Step 2.

### STEP 2

This step happens only when Target ASN(b) is the entity triggering AR/MAG migration during Idle Mode. The Target ASN (new AR/MAG) sends *Anchor\_DPF\_HO\_Trigger* to the Anchor PC-ASN(c) to indicate the AR/MAG Relocation.

### STEP 3

The Anchor PC sends *Anchor\_DPF\_HO\_Trigger* to the Anchor ASN(a) (old AR/MAG) to initiate the AR/MAG relocation process. The step MAY happen in response to the AR/MAG relocation trigger received in Step 2, if Target ASN(b) was the entity initiating the IM handover.

### STEP 4-11

PMIP6 CSN MM Handover procedure is performed as described in section 4.8.5.5. The PMIP6 IP session Context is transferred from Anchor ASN(a) to the Target ASN(b) which hosts the new AR/MAG, if not already obtained in the prior steps.

### STEP 12

If the Target ASN(b) (new AR/MAG) and Anchor PC are not collocated then Anchor ASN(a) (old AR/MAG) updates the Anchor PC with the *Context\_Rpt* message, confirming the AR/MAG relocation has happened. Anchor ASN includes the new Anchor ASN GW ID TLV in the *Context\_Rpt* message (Table 4-188).



## STEP 13

The Anchor PC-ASN sends *Context\_Ack* to Anchor ASN (old AR/MAG) and updates the MS related context with the new AR/MAG for the MS.

**Table 4-188 – Context\_Rpt from Anchor ASN (Old) to Anchor PC for PMIP6 IM handover**

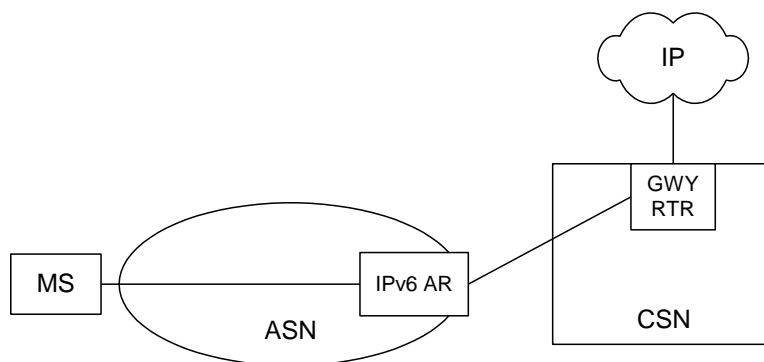
IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Context Purpose Indicator	5.3.2.36	M	Set to retrieval of the Anchor MM Context
MS Info	5.3.2.103	M	
>Service Authorization Code	5.3.2.181	O	
>Anchor ASN GW ID	5.3.2.10	M	Identifies the node that hosts the new Anchor DPF (i.e., PMIP6 AR/MAG) after the IM handover is completed.

## 4.11 IPv6

IPv6 in WiMAX can be operated in multiple ways. The packet convergence sublayer (CS) specified in the IEEE 802.16d/e specification is used for transport of all packet based protocols such as Internet protocol, IEEE Std 802.3/Ethernet and, IEEE Std 802.1Q. IPv6 can be run over the IP specific part of the packet CS or alternatively over the Ethernet (802.3/802.1Q) specific part of the packet CS. The operation of IPv6 over the IP specific part of the Packet CS is specified in [90] and should be referred to for understanding the basic mechanism. This section provides additional information about IPv6 operation that is WiMAX specific. IPv6 over 802.3 and 802.1Q specific parts of the packet CS are described in [87]. It should be noted that only the IP specific part of the packet CS is a mandatory requirement and support for 802.3 and 802.1Q parts of the packet CS is optional.

### 4.11.1 Network Model

The default IPv6 router or 1<sup>st</sup> hop router from the MS perspective is the access router in the ASN. The AR is an entity that resides in an ASN-GW. In case of network-based mobility management with PMIP6, the AR embeds the corresponding ASN's IP mobility function (Mobile Access Gateway - MAG). The MS autoconfigures an address based on the prefix advertised by the AR or is assigned an address via DHCPv6. This address is based on the prefix that topologically may belong to the Home CSN of the MS, or the Visited CSN which is directly attached to the ASN, if existing (for details see stage 2 section 7.2.2.2). This address is a globally routable address. The routability of this address is via the CSN that anchors the MS. Figure 4-170 shows the network model for IPv6.



**Figure 4-170 – IPv6 Network Model**

### 4.11.2 Point to Point Link Between the MS and AR

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 part of the packet CS. The combination of the transport connection over the air-interface (MS-BS, i.e., R1) and the L2 tunnel (GRE) over the R6 interface, between the BS and AR forms the point-to-point link. With the point-to-point type of link underlying the IPv6 layer, each MS is assigned one or more unique IPv6 prefixes. The only entities on the link are the MS and the AR. The granularity of the GRE tunnel between the BS and AR SHALL be on per SF basis.

The anchor data path function in the AR interfaces with the Anchor paging controller for paging an MS when needed.

### 4.11.3 IPv6 Link Establishment

The mobile station performs initial network entry as described in [refer to network entry procedure in section 4.5]. The subscriber profile is downloaded to the ASN as part of the successful completion of the network entry procedure.

On completion of the network entry procedure, the initial service flow (ISF) for IPv6 is established by the network. 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 unique transport connection identifier over the air interface. The ISF establishment procedure is described in section 4.6.4.2]. The trigger or decision to establish the IPv6 ISF is based on the subscriber's profile, network capability negotiation involving ASN, VCSN and HCSN, and indication by the MS in the SBC-REQ message (capability exchange). It is controlled by the SFA in the ASN.

The establishment of the IPv6 ISF enables the sending and receiving of IPv6 packets between the MS and the access router in the ASN. On completion of the establishment of the ISF, router advertisements and address assignment procedures are initiated. The successful establishment of the IPv6 ISF can be viewed as the trigger for the AR to send the router advertisement. The MS may also simultaneously send a router solicitation. The AR can be configured to send zero or more router advertisements on establishment of the IPv6 ISF. The RADIUS Access-Accept message or Diameter WDEA command received by the ASN during the authentication phase MAY contain one or more Framed-IPv6-Prefix attributes/AVPs (for PMIPv6 service separate RADIUS attributes SHALL be used to bootstrap the HNP information). In this case the AR SHALL use that prefix(es) to populate the Prefix Information option(s) in the Router Advertisement message sent to the MS. If the Access-Accept AAA message does not contain Framed-IPv6-Prefix attribute/AVP, the ASN SHALL advertise a prefix from a preconfigured pool of prefixes belonging to the directly attached CSN. In case of a NAP sharing, the ASN may have several different prefix pools associated with different CSN. In such case the ASN SHALL use the realm part of the MS NAI to select an appropriate pool.

An MS receives an RA from the AR on completion of the establishment of the IPv6 ISF. An MS may also send router solicitations on completion of the establishment of the ISF. If the MS does not receive an unsolicited RA from the AR or in response to a router solicitation, the MS will initiate network exit and re-entry procedures.

An MS can have multiple IPv6 service flows with different QoS characteristics. However the IPv6 ISF can be considered as the primary service flow. The concept of the ISF is described in [refer to section 4.6.4.2]. The ASN

GW/AR treats each ISF, along with the other service flows to the same MS, as a unique link and manages it as a separate (virtual) interface per link.

The IPv6 prefix assigned to an MS may be used as the classifier at the AR for the downlink associated with the MS. Finer grain classifiers which may include the complete IPv6 address and/or port numbers can be established as well.

#### 4.11.4 Address Configuration

The addressing scheme for IPv6 hosts in WiMAX follows the IETF recommendation for hosts specified in [31]. The IPv6 node requirements RFC specifies a set of RFCs that are applicable for addressing. These include:

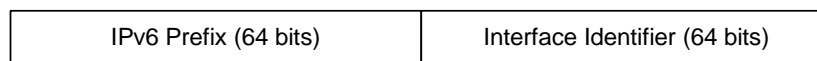
- IPv6 Addressing Architecture – [49] (Updated by [58])
- IPv6 stateless address autoconfiguration – [78]
- Privacy Extensions for Address Configuration in IPv6 – [43]
- Default Address Selection for IPv6 – RFC 3484
- Stateful Address Autoconfiguration – DHCPv6, [47]

The node requirements [31] specify which of the above addressing related RFCs are mandatory to implement and which are optional.

##### 4.11.4.1 Interface Identifier (IID)

The MS has a 48-bit MAC address as specified in [Ref1]. This MAC address is used to generate the 64 bit interface identifier which is used by the MS for address autoconfiguration. The IID is generated by the MS as specified in RFC2464.

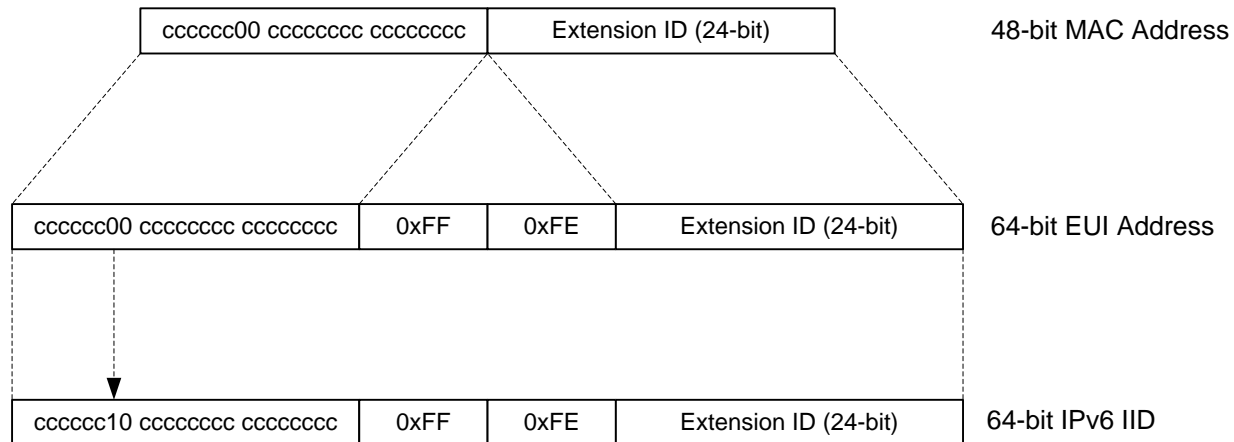
IPv6 address is formed by adding an Interface Identifier (IID) to the prefix learnt from Router Advertisement. The IID forms the least significant bits of the IPv6 address as shown below:



**Figure 4-171 – IPv6 Address Format**

The length of the IID is fixed and SHALL be 64-bits for all nodes in the WiMAX Network.

The IID for 802.16 interfaces is based on the EUI-64 identifier derived from the interface's built-in 48-bit MAC address. EUI-64 bit identifier is formed by inserting 0xFFFE in the MAC address between the company ID (first 24 bits) and the manufacturer selected extension ID (last 24 bits). The IID is then formed from the EUI-64 by inverting the universal/local (u/l) bit. This is the 7th bit of the most significant octet. Inverting this bit will generally change a 0 value to a 1 meaning globally unique IPv6 IID.



**Figure 4-172 – Illustration of Forming the IID**

For addresses that are based on privacy extensions, the MS may generate random IIDs as specified in RFC3041.

#### 4.11.4.2 Duplicate Address Detection (DAD)

DAD is performed as per RFC 2461, [27].

#### 4.11.4.3 Stateless Address Auto-configuration

Stateless address auto-configuration is performed as per RFC 2461, [27]. The access router in the ASN is the default router that advertises a prefix that is used by the MS to configure an address.

#### 4.11.4.4 Stateful Address Auto-configuration

If the M-flag is set in the RA message from the access router to the MS, the MS MAY perform stateful address autoconfiguration. For this purpose, the MS SHALL use DHCPv6 procedures as defined in [47]. The MS SHALL send the DHCP request message to the all-nodes DHCP server or all-nodes DHCP relay addresses. The ASN-GW/AR acts as the DHCP-server (proxy) or DHCP-relay to assist the MS to acquire an IPv6 address in a stateful manner. If acting as a DHCP relay, the ASN-GW SHALL follow the relay procedures defined in [47].

#### 4.11.5 DNS Discovery

In order to be able to use the Domain Name Service (DNS), the MS has to be configured with the IPv6 DNS server addresses. The IPv6 specified standard mechanism for dynamically configuring the DNS server addresses is via Dynamic Host Configuration Protocol (DHCP) for IPv6 using DNS Configuration options [Reference to RFC 3646].

Choosing the right DNS Server configuration method is dependent on the address allocation mechanisms. If stateful address auto-configuration is used; then DHCPv6 DNS Configuration options SHALL be used. However, when using stateless address auto-configuration, well-known addresses, or stateless DHCPv6 [RFC3736] SHALL be used.

##### 4.11.5.1 DHCPv6 DNS Configuration Options

The DHCPv6 DNS configuration options are defined in [RFC3646]. The DNS recursive name server options SHALL be populated by the network's name server addresses. In addition, the Domain search list option MAY be present and populated with the network's search list.

The MS MAY use DHCPv6 DNS Configuration Options [RFC3646] – either with DHCPv6 [47] when stateful address configuration is used, or Stateless DHCPv6 [RFC3736] when stateless address auto-configuration is used.

The network SHALL support DHCPv6 [47] and DHCPv6 DNS Configuration Options [RFC3646] when stateful address auto-configuration, is used. The network SHALL support stateless DHCPv6 [47] with the DNS Configuration options [RFC3646] when stateless address auto-configuration is used.

## **4.11.6 Uplink and Downlink Transmission of IPv6 Packets**

### **4.11.6.1 Uplink**

IPv6 packets can be sent by the MS over the IP specific part of the Packet CS with IPv6 classifiers, via a transport connection that maps to either the IPv6 Initial service flow or to another IPv6 pre-provisioned service flow in the ASN. The MS sends IPv6 packets that are carried over a transport connection identified by a connection Identifier (CID). The IP specific part of the packet CS at the BS receives the IPv6 packet. Based on the CID that the packet 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 Data path ID (GRE key) to send the packet to the Access router (AR) via the GRE tunnel (R6).

### **4.11.6.2 Downlink**

When a packet destined for an MS arrives at the AR, the AR looks at the IPv6 packet header and/or flow ID to determine the service flow ID (SFID) that this packet needs to be mapped on to. The SFID maps to a data path ID. The ASN GW uses the GRE key associated with the data path ID to forward the IPv6 packet via the GRE tunnel to the BS. When the BS receives the IPv6 packet the BS forwards the IPv6 packet on a transport connection identified by a CID to the appropriate MS using the mapping of the SFID to the transport connection. The BS may also utilize the IPv6 classifiers to determine the transport connection to be used for sending the packet.

## **4.11.7 IPv6 AR Relocation (R3 relocation)**

Relocation of the IPv6 AR causes the MS to be assigned a new prefix and hence a new address. However, in case of PMIPv6 the MS retains the same Home Network Prefix even after AR/MAG relocation allowing it to maintain its current IP session. The decision to relocate the AR for an MS is determined by a functional entity in the ASN. AR relocation also causes the MS to update its binding with an HA in the case of Mobile IPv6. The decision to relocate the AR for an MS is always controlled by the network. The types of triggers that can cause AR/R3 relocation are:

- a. MS mobility: The MS hands off to a new Base Station under a new Access Router.
- b. Wake-up from idle mode: The MS wakes up from the idle mode under a different Access Router than the one under which it entered the idle mode.
- c. Resource optimization: The network decides for resource optimization purposes to transfer the R3 endpoint for the MS from the serving Access Router to a new Access Router.

AR relocation for an MS requires the MS to perform network re-entry procedure in the scenario the MS wakes up from Idle mode and receives an RA with a prefix that is different from the one it previously had received. In case of R3 relocation as a result of MS mobility and/or resource optimization reasons, network re-entry is not required. The classifier associated with the service flows will however have to be updated with the new prefix. AR relocation can be triggered when the MS is in active mode or in Idle mode.

## 4.12 Utility Call Flows

The following sections describe specify commonly used R4 call flows and referenced by other sections in this specification.

### 4.12.1 Data Path Pre-Registration Procedure

#### 4.12.1.1 R4/R6 Data Path Pre-Registration Procedure

The following call flow describes the R4/R6 Data Path Pre-Registration procedure. Data Path Pre-Registration may be initiated by the Target BS(s).

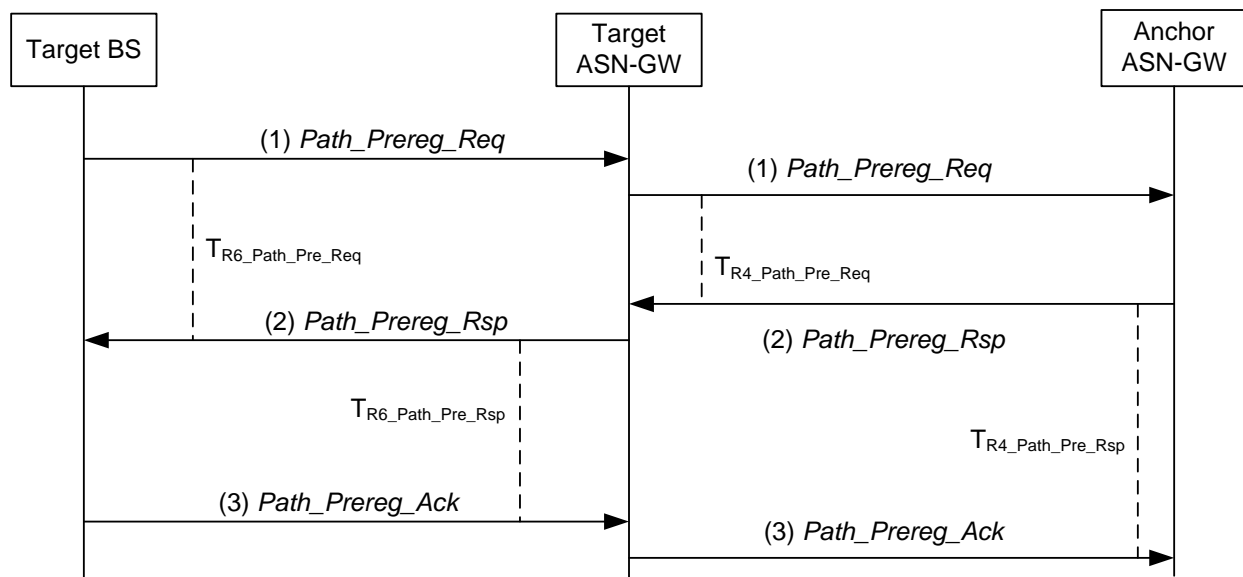


Figure 4-173 – R4/R6 Data Path Pre-Registration Procedure

#### STEP 1

Target BS initiates pre-establishment of the data path for an MS by sending a *Path\_Prereg\_Req* message which includes the data path information to the Target ASN GW and starts timer  $T_{R6\_Path\_Pre\_Req}$ .

The Target ASN-GW initiates pre-establishment of the data path for an MS by sending an R4 *Path\_Prereg\_Req* message which includes the data path information to the Anchor ASN-GW and starts timer  $T_{R4\_Path\_Pre\_Req}$ .

#### STEP 2

The Anchor ASN-GW sends a *Path\_Prereg\_Rsp* message to the Target ASN-GW and starts timer  $T_{R4\_Path\_Pre\_Rsp}$ . Upon receipt of the *Path\_Prereg\_Rsp* message, the Target ASN-GW stops timer  $T_{R4\_Path\_Pre\_Req}$ .

The Target ASN GW sends a *Path\_Prereg\_Rsp* message to the Target BS and starts timer  $T_{R6\_Path\_Pre\_Rsp}$ . Upon receipt of the *Path\_Prereg\_Rsp* message, Target BS stops timer  $T_{R6\_Path\_Pre\_Req}$ .

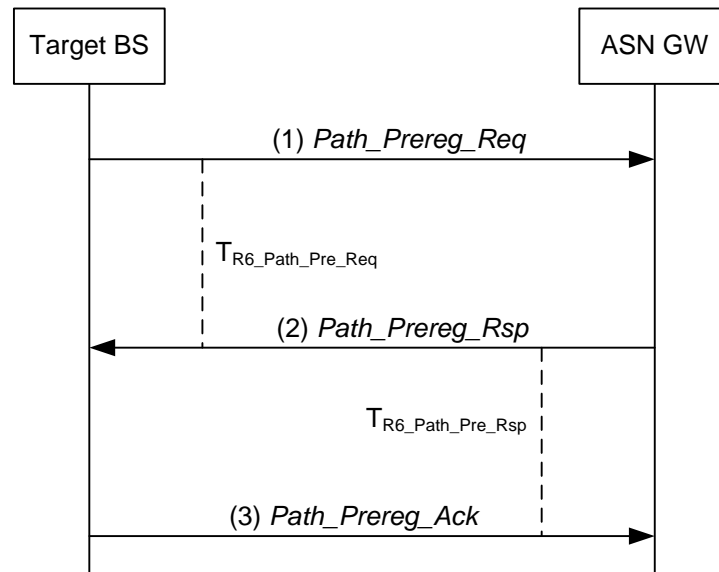
#### STEP 3

The Target BS sends a *Path\_Prereg\_Ack* message to the Target ASN-GW. Upon receipt of the *Path\_Prereg\_Ack* message, the Target ASN GW stops timer  $T_{R6\_Path\_Pre\_Rsp}$ .

The Target ASN-GW sends a *Path\_Prereg\_Ack* message to the Anchor ASN-GW. Upon receipt of the *Path\_Prereg\_Ack* message, the Anchor ASN-GW stops timer  $T_{R4\_Path\_Pre\_Rsp}$ .

#### 4.12.1.2 R6 Data Path Pre-Registration Procedure

The following call flow describes the R6 Path Pre-Registration procedure during handovers. Data Path Pre-Registration is initiated by the Target BS(s).



**Figure 4-174 – R6 Data Path Pre-Registration Procedure**

##### STEP 1

Target BS initiates pre-establishment of the data path for an MS by sending a *Path\_Prereg\_Req* message to ASN GW and starts timer  $T_{R6\_Path\_Pre\_Req}$ .

##### STEP 2

ASN GW sends a *Path\_Prereg\_Rsp* message to the Target BS and starts timer  $T_{R6\_Path\_Pre\_Rsp}$ . Upon receipt of the *Path\_Prereg\_Rsp* message, Target BS stops timer  $T_{R6\_Path\_Pre\_Req}$ .

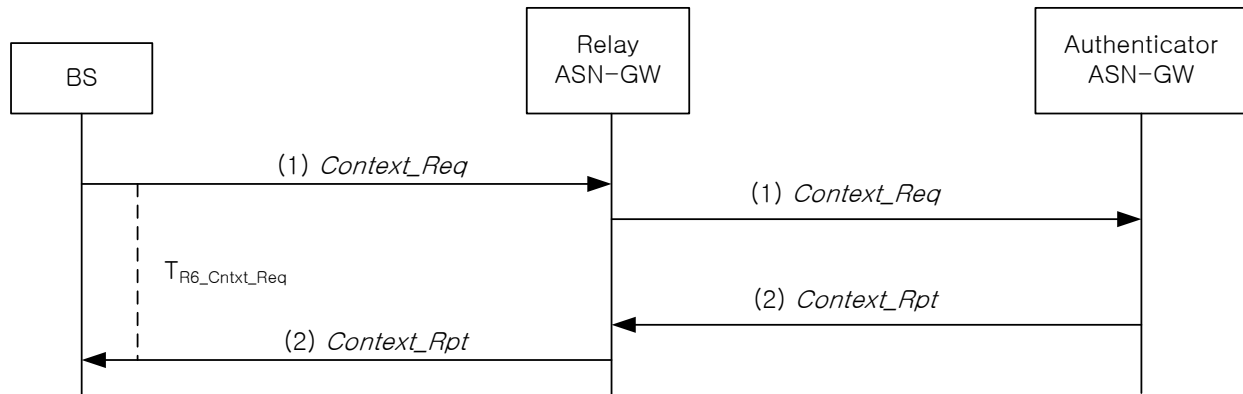
##### STEP 3

Target BS sends a *Path\_Prereg\_Ack* message to ASN GW. Upon receipt of the *Path\_Prereg\_Ack* message, ASN GW stops timer  $T_{R6\_Path\_Pre\_Rsp}$ .

## 4.12.2 Context Retrieval Procedure

### 4.12.2.1 R4/R6 Context Retrieval Procedure

The following call flow describes the Context Retrieval procedure. A Serving or Target BS MAY initiate this procedure to request AK context information for a mobile from an Authenticator ASN-GW. A Target BS MAY also use this procedure to request the most recent MAC context from the Serving ASN.



**Figure 4-175 – R4/R6 Context Retrieval Procedure**

#### STEP 1

BS sends a *Context\_Req* message to the Authenticator ASN GW to request the stored context associated with a specified MS. The ASN GW starts timer  $T_{R6\_Cntxt\_Req}$ .

The Relay ASN-GW relays a *Context\_Req* message to the Authenticator ASN-GW to request the stored context associated with a specified BS.

If the Relay ASN-GW is functioning in a relay mode, it SHALL not start timer  $T_{R4\_Cntxt\_Req}$ .

#### STEP 2

The Authenticator ASN-GW responds by sending the requested context information for the mobile in the *Context\_Rpt* message.

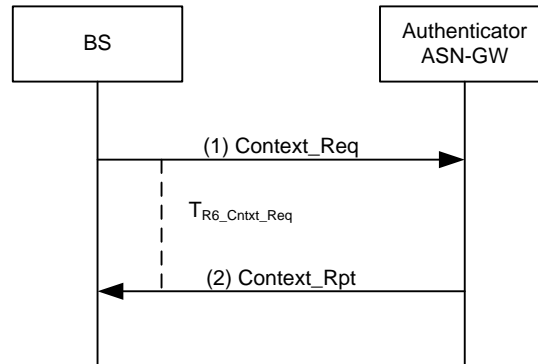
If BS receives response with the result code "Partial Response" it can request the missing info or continue processing assuming that other responses are not available; If BS receives response with code "Multiple not supported" it can request the missing info in a single new request, multiple new requests one-by-one or continue processing with a single information element without asking for more information - the decision is up to local policies.

Authenticator ASN GW responds by sending the requested context information for the mobile in the *Context\_Rpt* message. The Relay ASN-GW relays the message over R4/R6. Upon receipt of the *Context\_Rpt* message, ASN-GW stops timer  $T_{R4\_Cntxt\_Req}$  and BS stops timer  $T_{R6\_Cntxt\_Req}$ , respectively.



#### 4.12.2.2 R6 Context Retrieval Procedure

The following call flow describes the R6 Authenticator Context Retrieval procedure from an authenticator located in the local ASN-GW (i.e., an ASN GW which has R6 interface with the BS). If not located locally, the R6 *Context\_Req* and *Context\_Rpt* messages will be further relayed by the local ASN-GW over R4 to the Anchor Authenticator.



**Figure 4-176 – R6 Authenticator Context Retrieval Procedure**

##### STEP 1

BS sends a *Context\_Req* message to the Authenticator ASN GW to request the stored context associated with a specified MS. The ASN GW starts timer  $T_{R6\_Cntxt\_Req}$ .

##### STEP 2

Authenticator ASN GW responds by sending the requested context information for the mobile in the *Context\_Rpt* message. Upon receipt of the *Context\_Rpt* message, BS stops timer  $T_{R6\_Cntxt\_Req}$ .

### 4.12.3 Data Path Registration Procedure

#### 4.12.3.1 R4/R6 Data Path Registration Procedure

The following call flow describes the Data Path Registration procedure. The Data Path Registration procedure occurs between a Target BS and Anchor ASN-GW immediately after the MS has arrived at the Target BS.

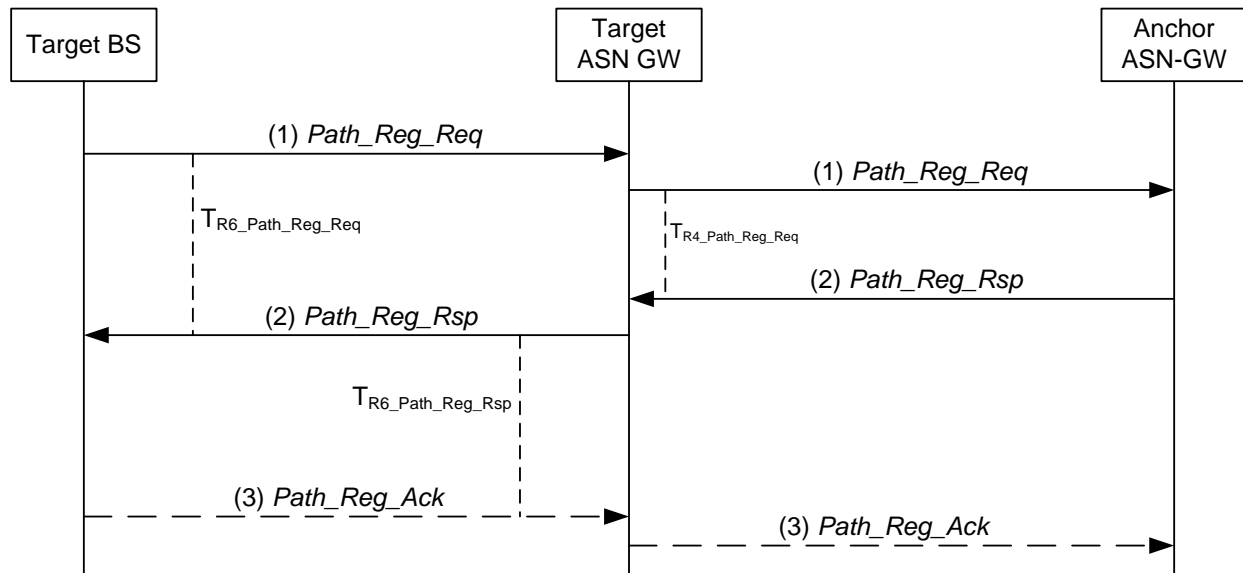


Figure 4-177 – R4/R6 Data Path Registration Procedure

#### STEP 1

Target BS initiates Data Path Registration procedure by sending a *Path\_Reg\_Req* message to the Target ASN- GW and starts timer T<sub>R6\_Path\_Reg\_Req</sub>.

Target ASN-GW initiates Data Path Registration procedure by sending a *Path\_Reg\_Req* message to Anchor ASN and starts timer T<sub>R4\_Path\_Reg\_Req</sub>.

#### STEP 2

Anchor ASN-GW sends a *Path\_Reg\_Rsp* message to Target ASN-GW. Anchor ASN-GW starts timer T<sub>R4\_Path\_Reg\_Rsp</sub>, if no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction. Upon receipt of the *Path\_Reg\_Rsp* message, Target ASN-GW stops timer T<sub>R4\_Path\_Reg\_Req</sub>.

The Target ASN GW sends a *Path\_Reg\_Rsp* message to Target BS and, if no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, starts timer T<sub>R6\_Path\_Reg\_Rsp</sub>. Upon receipt of the *Path\_Reg\_Rsp* message, Target BS stops timer T<sub>R6\_Path\_Reg\_Req</sub>.

#### STEP 3

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction then Target BS sends a *Path\_Reg\_Ack* message to ASN GW. Upon receipt of the *Path\_Reg\_Ack* message, ASN GW stops timer T<sub>R6\_Path\_Reg\_Rsp</sub>.

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction then Target ASN-GW sends a *Path\_Reg\_Ack* message to Anchor ASN-GW. Upon receipt of the *Path\_Reg\_Ack* message, Anchor ASN-GW stops timer T<sub>R4\_Path\_Reg\_Rsp</sub>.

#### 4.12.3.2 R6 Data Path Registration Procedure

Data Path Registration procedure takes place between the Target BS and ASN GW immediately after the MS has arrived at the Target BS.

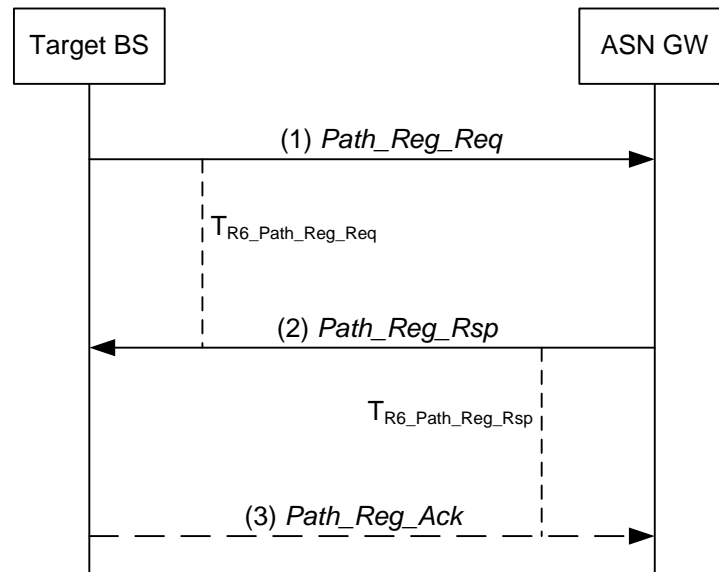


Figure 4-178 – Data Path Registration Procedure

##### STEP 1

Target BS initiates Data Path Registration procedure by sending a *Path\_Reg\_Req* message to ASN GW and starts timer T<sub>R6\_Path\_Reg\_Req</sub>.

##### STEP 2

ASN GW sends a *Path\_Reg\_Rsp* message to Target BS and, if no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, starts timer T<sub>R6\_Path\_Reg\_Rsp</sub>. Upon receipt of the *Path\_Reg\_Rsp* message, Target BS stops timer T<sub>R6\_Path\_Reg\_Req</sub>.

##### STEP 3

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction then Target BS sends a *Path\_Reg\_Ack* message to ASN GW. Upon receipt of the *Path\_Reg\_Ack* message, ASN GW stops timer T<sub>R6\_Path\_Reg\_Rsp</sub>.

## 4.12.4 R4 Data Path De-Registration Procedure

### 4.12.4.1 R4/R6 Data Path De-Registration Procedure

The following call flow describes the Data Path De-Registration procedure.

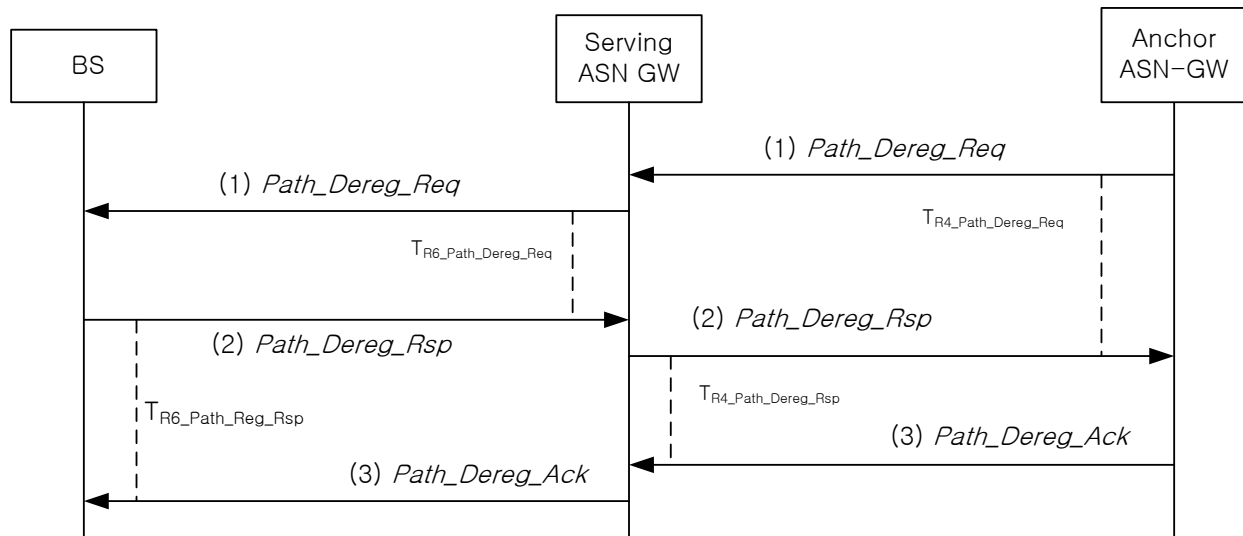


Figure 4-179 – R4/R6 Data Path De-Registration Procedure

#### STEP 1

Anchor ASN-GW initiates Data Path De-Registration procedure by sending a *Path\_Dereg\_Req* message to Serving ASN-GW and starts timer  $T_{R4\_Path\_De-Reg\_Req}$ .

Serving ASN-GW initiates Data Path De-Registration procedure by sending a *Path\_Dereg\_Req* message to BS and starts timer  $T_{R6\_Path\_De-Reg\_Req}$ .

#### STEP 2

BS sends a *Path\_Dereg\_Rsp* message to Serving ASN-GW and starts  $T_{R6\_Path\_De-Reg\_Rsp}$ . Upon receipt of the *Path\_Dereg\_Rsp* message, Serving ASN-GW stops timer  $T_{R6\_Path\_De-Reg\_Req}$ .

Serving ASN-GW sends a *Path\_Dereg\_Rsp* message to Anchor ASN-GW and starts timer  $T_{R4\_Path\_De-Reg\_Rsp}$ . Upon receipt of the *Path\_Dereg\_Rsp* message, Anchor ASN-GW stops timer  $T_{R4\_Path\_De-Reg\_Req}$ .

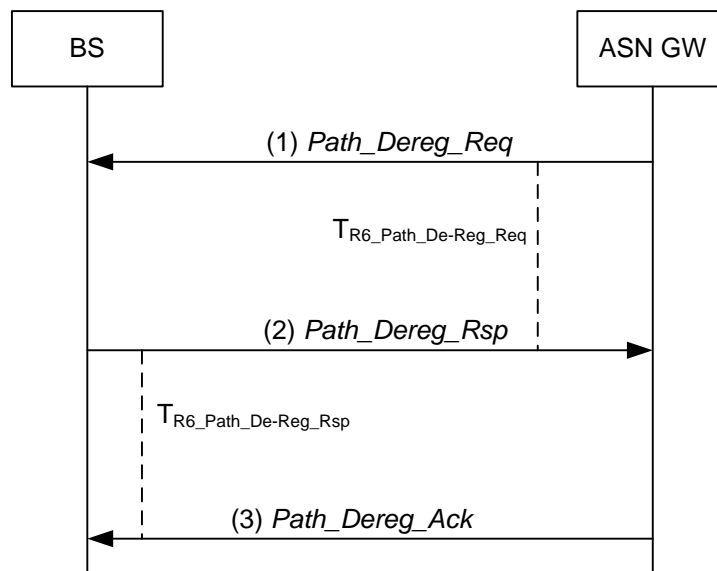
#### STEP 3

Anchor ASN-GW sends a *Path\_Dereg\_Ack* message to Serving ASN-GW. Upon receipt of the *Path\_Dereg\_Ack* message, Serving ASN-GW stops timer  $T_{R4\_Path\_De-Reg\_Rsp}$ .

Serving ASN-GW sends a *Path\_Dereg\_Rsp* message to BS. Upon receipt of the *Path\_Dereg\_Rsp* message, BS stops timer  $T_{R6\_Path\_De-Reg\_Rsp}$ .

#### 4.12.4.2 R6 Data Path De-Registration Procedure

Path De-Registration Procedure is shown in Figure 4-180.



**Figure 4-180 –Path De-Registration Procedure**

##### STEP 1

ASN GW initiates Data Path De-Registration procedure by sending a *Path\_Dereg\_Req* message to BS and starts timer  $T_{R6\_Path\_De-Reg\_Req}$ .

##### STEP 2

BS sends a *Path\_Dereg\_Rsp* message to ASN GW and starts timer  $T_{R6\_Path\_De-Reg\_Rsp}$ . Upon receipt of the *Path\_Dereg\_Rsp* message, ASN GW stops timer  $T_{R6\_Path\_De-Reg\_Req}$ .

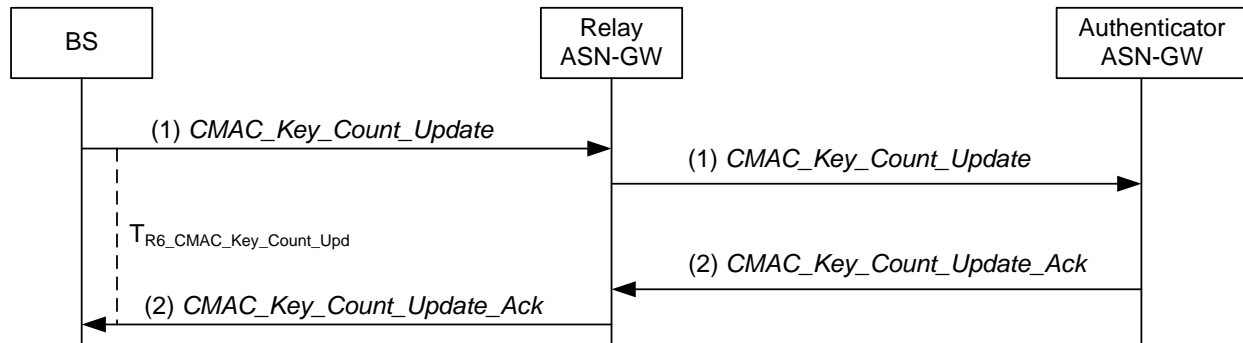
##### STEP 3

ASN GW sends a *Path\_Dereg\_Ack* message to BS. Upon receipt of the *Path\_Dereg\_Ack* message, BS stops timer  $T_{R6\_Path\_De-Reg\_Rsp}$ .

## 4.12.5 CMAC Key Count Update Procedure

### 4.12.5.1 R4/R6 CMAC Key Count Update Procedure

The following call flow describes the R4/R6 CMAC Key Count Update procedure.



**Figure 4-181 – R4/R6 CMAC Key Count Update Procedure**

#### STEP 1

Target (New Serving) BS initiates CMAC Key Count Update procedure by sending a *CMAC\_Key\_Count\_Update* message to ASN-GW and starts timer  $T_{R6\_CMAC\_Key\_Count\_Upd}$ . If the Serving ASN-GW is not hosting the Authenticator for the MS, it will forward this message to the Authenticator ASN-GW via the *CMAC\_Key\_Count\_Update* message.

The Relay ASN-GW relays the CMAC Count Update procedure by sending a *CMAC\_Key\_Count\_Update* message to the Authenticator ASN-GW.

If the Relay ASN-GW is functioning in a relay mode, it SHALL not start timer  $T_{R4\_CMAC\_Key\_Count\_Upd}$ .

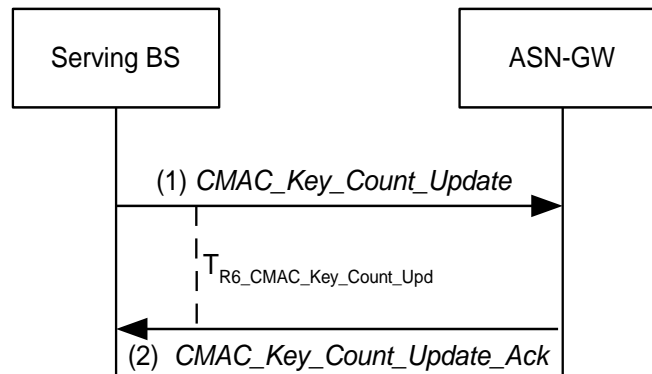
#### STEP 2

The Authenticator ASN-GW updates the key count for the MS, then sends a *CMAC\_Key\_Count\_Update\_Ack* message to BS. The Relay ASN-GW relays the message to the BS. Upon receipt of the *CMAC\_Key\_Count\_Update\_Ack* message, Relay ASN-GW stops timer  $T_{R4\_CMAC\_Key\_Count\_Upd}$  and BS stops timer  $T_{R6\_CMAC\_Key\_Count\_Upd}$  respectively.

Please note that when the Authenticator and Anchor ASN are co-located, the CMAC Count Update exchange can be piggybacked to the R4 *Path\_Reg\_Req* and *Path\_Reg\_Rsp* exchange. Such Piggybacking can be accomplished only after the mobile enters the network.

#### 4.12.5.2 R6 CMAC Key Count Update Procedure

The following call flow describes the R6 CMAC Key Count Update procedure.



**Figure 4-182 – R6 CMAC Key Count Update Procedure**

##### STEP 1

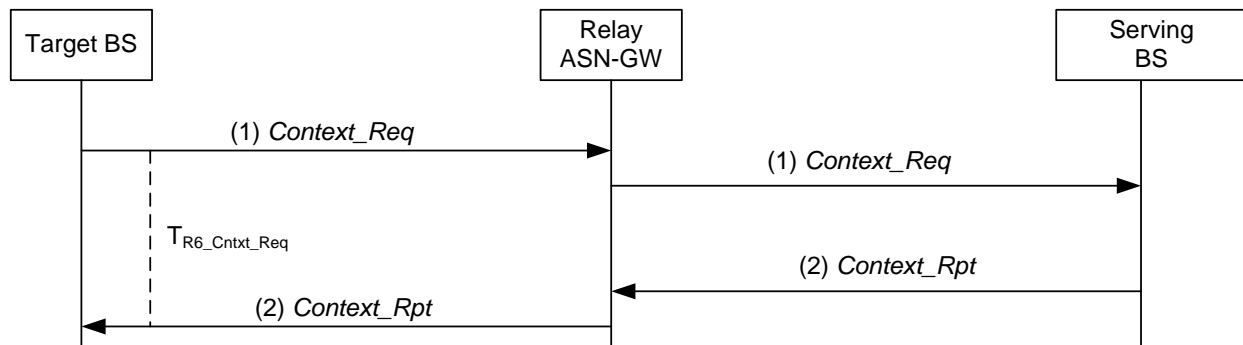
A Serving BS initiates the R6 CMAC Key Count Update procedure by sending an R6 *CMAC\_Key\_Count\_Update* message to the ASN-GW and starts timer  $T_{R6\_CMAC\_Key\_Count\_Upd}$ .

##### STEP 2

Upon successfully updating the Authenticator ASN with the new key count, the ASN-GW sends an R6 *CMAC\_Key\_Count\_Update\_Ack* message to the Serving BS. Upon receipt of the R6 *CMAC\_Key\_Count\_Update\_Ack* message, the Serving BS stops timer  $T_{R6\_CMAC\_Key\_Count\_Upd}$ .

#### 4.12.6 MAC Context Retrieval Procedure

MAC Context Retrieval Procedure is shown in the following figure.



**Figure 4-183 – MAC Context Retrieval Procedure**

##### STEP 1

Target BS sends a *Context\_Req* message to request the context associated with a specified MS stored in the Serving BS. The Target BS starts timer T<sub>R6\_Cntxt\_Req</sub>.

##### STEP 2

Relay ASN GW relays the message to the Serving BS.

##### STEP 3

Serving BS responds by sending the requested context information for the mobile in the *Context\_Rpt* message.

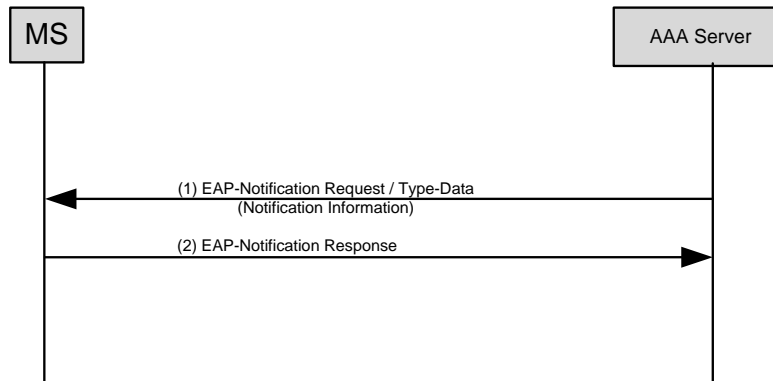
##### STEP 4

Relay ASN GW relays the message to the Target BS. Upon receipt of the *Context\_Rpt* message, Target BS stops timer T<sub>R6\_Cntxt\_Req</sub>.



#### 4.12.7 EAP Notification Exchange

This section describes the EAP notification procedure that MAY be initiated by the AAA server to convey notification information to the MS. As part of an EAP method exchange, the notification exchange is embedded in the overall EAP method exchanges as defined in section 4.5.1.1.



**Figure 4-184 – EAP notification exchange**

##### STEP 1

The AAA server sends an *EAP-Notification Request* message to the MS including the Notification Information coded in the Type-Data field of the EAP-Notification message.

##### STEP 2

The MS acknowledges the reception of the *EAP-Notification Request* message with the *EAP-Notification Response* message.

**Table 4-189 – Type-Data field of the EAP Notification Request packet**

Element Name	Length in octets	Description	M/O
Human Readable String	Variable	If required, UTF-8 encoded human readable message MAY be included prior to the NULL character. Then, the MS SHOULD display this message to the user if the integrity check succeeds.	O
Delimiter	1	The NULL character (0x00)	M
Notification Information String	Variable	ASCII string that is BASE64-encoded from the Notification Information TLV described in the Section 5.8.1. The MS SHOULD NOT display this string to the user as it is, without proper translation.	O <sup>3</sup>
Network Rejection Information String	Variable	ASCII string that is BASE64-encoded from the Network Rejection Information TLV described in the Section 5.8.3. The MS SHOULD NOT display this string to the user as it is, without proper translation.	O <sup>4</sup>

Note 1: Due to the limitations imposed by the EAP-Notification message transport the total Type-Data field SHALL NOT exceed 1015 Octets, including the Notification Information String element.

Note 2: The format of the Type-Data field described above SHALL be applied only in the Network Rejection Procedure or, i.e., when the EAP-Notification Request is used to deliver the Network Rejection Information.

Note 3: This field SHALL be present whenever the EAP notification is sent to provide BS ID List where a MS is allowed for network entry.

Note 4: This field SHALL be present whenever the EAP notification is sent as part of a network rejection procedure.

### 4.13 Simple IP Management

This section describes procedures between the MS, ASN and CSN related to establishment and management of MS' IP layer connectivity in the Simple IP mode.

During access authentication procedure ASN, VCSN (if present) and HCSN SHALL exchange their network service capabilities and negotiate the type of network service to be provided to the MS. Depending on the outcome of service negotiation process, Simple IPv4 or Simple IPv6 services may be setup after successful access authentication. If more than one IP service is authorized, the provided IP service is based on local ASN policies and terminal capabilities (e.g. IPv6 and/or IPv4).

The user plane traffic of simple IP MSs between the ASN and the CSN SHALL be delivered over existing data path. The exact type of the data path and mechanism used for path establishment are not defined by this specification. It is expected that the data path is established and maintained as per bilateral agreements between the WiMAX operators.

In the roaming case simple IP service can either be provided by the visited CSN or by the home CSN of the MS. The selection of the designated CSN providing the simple IP service in such case is subject to the agreements between operators. There must be a simple IP data path between ASN and the CSN, which is providing the IP services. In case of roaming with split ASN and CSN and IP services provided by the HCSN, the Simple IP data path must traverse the VCSN. This data path may also traverse the VCSN when not directly providing a simple IP service to the MS.

#### 4.13.1 AR requirements

Access Router (AR) is the 1st hop IP router for the MS and is acting as a default gateway for the MS. The AR functionality is located in the ASN GW.

AR SHALL have a data path with the CR in the CSN. AR MAY have several data paths for simple IP service and each of these data paths MAY be terminated by a different CSN owned by a different operator.

AR SHALL use the domain part of the MS NAI and match it with the operator name of the CSN to select the right data path over which the MS user plane SHALL be delivered to the CSN.

AR SHALL deliver all uplink traffic from the simple IP MS to the CSN via a data path. When the AR receives an uplink packet from the BS, it MAY use the GRE key ID of the GRE tunnel over which it received the packet to retrieve the MS context and then deliver the packet over the data path contained in the MS context.

AR SHALL receive downlink MS traffic from the CSN via a data path. AR MAY use the destination IP address of the downlink packet to locate the MS context. If no matching MS context is found, the AR SHALL discard the received downlink packet. In case private IP addresses are used, it may happen that there are several MSs using the same IP address. The AR SHALL support MSs with overlapping private IP addresses and SHALL deliver packets to the appropriate MS based on corresponding CSN data path which the MS is associated with.

While in active mode, the AR function handling the MS traffic cannot be changed or relocated for the duration of the MS IP session.

#### 4.13.2 CR requirements

Core Router (CR) is a functional entity located in the CSN that terminates the simple IP data path from the ASN. CR is a topological anchor for the MS IP address. It intercepts packets destined for the MS and delivers them to the ASN where the MS is located.

CR SHALL have a data path with the AR. CR MAY have several data paths for simple IP service and each of those data paths MAY be terminated by a different ASN owned by a different operator.

CR SHALL deliver all downlink traffic for the simple IP MS to the ASN where the MS is attached via the data path.

CR SHALL receive uplink MS traffic from the ASN where the MS is attached via the data path.

#### **4.13.3 AAA server requirements**

AAA server SHALL authorize specific IP service(s) and provide configuration information as a result of matching the ASN/CSN IP service capabilities, the subscriber profile and the network policy. In case of successful access authentication, the RADIUS Access-Accept packet or Diameter WDEA command SHALL carry authorized Network services information, configuration parameters corresponding to the Authorized Network Services (or Visited Authorized Network Services).

The AAA servers (VAAA or HAAA) MAY deliver an IP address to be assigned to the MS in the RADIUS Access-Accept packet or Diameter WDEA command indicating successful access authentication. When assigned by the VAAA or HAAA, the IP address is released in the AAA when RADIUS Accounting-Request Stop (release indication) or Diameter WSTR command is sent from the ASN to the AAA-server. The AAA server(s) may deliver both IPv4 address and IPv6 prefix and IPv6 interface id in the same message. The IPv4 address assigned by the home-CSN or visited-CSN is respectively carried in the Framed-IP-Address or Visited-Framed-IP-address attribute. IPv6 prefix and Interface-Id assigned by the home CSN are carried in the Framed-IPv6-Prefix attribute and Framed-IPv6-Interface-Id, IPv6 prefix and Interface Id assigned by the visited CSN are carried in the Visited-Framed-IPv6-Prefix and Visited-Framed-Interface-Id. The IPv6 prefix in Framed-IPv6-Prefix or Visited-Framed-IPv6-Prefix attributes SHALL be unique to this MS. The AAA server(s) SHALL NOT allocate an IPv6 prefix whose valid/preferred lifetime is less than the Session-Timeout attribute value. For example, if a prefix will expire in 1 day, it SHALL NOT be used with a Session-Timeout value greater than 1 day.

For IPv6, the VAAA MAY include the Visited-Framed-Interface-Id and the Visited-Framed-IPv6-Prefix attribute in the RADIUS Access-Request or Diameter WDER command to be forwarded to HAAA, if local network policy allows.

The HAAA may decide based on local network policies to remove or echo the Visited-Framed-Interface-Id and the Visited-Framed-IPv6-Prefix attribute in the AAA Access-Accept packet. The final RADIUS Access-Accept packet or Diameter WDEA may include the following attributes: Framed-Interface-Id and/or Visited-Framed-Interface-Id, and Framed-IPv6-Prefix and/or Visited-Framed-IPv6-prefix.

For IPv4, the VAAA may include the Visited-Framed-IP-Address attribute in the RADIUS Access-Request packet or Diameter WDER command to be forwarded to HAAA, if local network policy allows.

The HAAA may decide based on local network policies to remove or echo the Visited-Framed-IP-Address attribute in the RADIUS Access-Accept packet or Diameter WDEA command. The final RADIUS Access-Accept packet or Diameter WDEA command may include the following attributes: Framed-IP-Address and/or Visited-Framed-IP-Address.

During the access authentication phase, the VAAA or HAAA server MAY assign a v-DHCP or h-DHCP server respectively located in the CSN to be used for the MS IP configuration. The assigned DHCP server address is carried in the final RADIUS Access-Accept packet or Diameter WDEA command and is used by the DHCP relay in the ASN as a destination to which DHCP messages from the client are relayed.

#### **4.13.4 Requirements specific to Simple IPv4 service**

This section specifies additional requirements that are specific to the simple IPv4 service.

##### **4.13.4.1 MS Requirements**

The MS SHALL support requirements as defined in sections 4.8.2.1.1 (requirements related to session establishment), section 4.8.2.2.1 (requirements related to session renewal) and section 4.8.2.4.1 (requirements related to session release).

##### **4.13.4.2 DHCP Requirements**

The ASN-GW SHALL support DHCP Proxy. The ASN-GW MAY also support DHCP Relay.

#### 4.13.4.2.1 DHCP Proxy requirements

Upon receiving a DHCPDISCOVER message from the MS, the DHCP proxy MAY ignore the “chaddr” field in the DHCP header and client-identifier DHCP option and use the Outer-Identity associated with the ISF data path tunnel over which the DHCP message was received as the identity of the MS. This is done to prevent MAC address spoofing by a rogue MS.

In case the DHCP proxy determines that the MS has included a MAC address in the chaddr field or client-identifier option that is not matching with the known MAC address associated with the data path over which the DHCP message is received, the DHCP proxy MAY consider the following:

- A rogue MS trying to spoof MAC address. In this case, the DHCP proxy MAY inform the DPF to initiate data path, i.e., R6 teardown.

The DHCP proxy SHALL use the extracted MS Identity (Outer-Identity associated with ISF or MAC address) to locate the MS info in the NAS. If the MS info contains an MS address, it will be used to respond back to the MS with a DHCPOFFER message setting the yiaddr(address) field to the MS address as received from AAA server. If the framed address from both VCSN and HCSN is available, then an anchor selection mechanism needs to be executed to select the anchor CSN for the data path. The details of this mechanism are outside the scope of this specification. DHCP Proxy MAY set the subnet option to the value indicated in the Framed-IP-Netmask attribute, in case such attribute is contained in the NAS. The DHCP proxy SHALL set the Subnet option to the value 255.255.255.255 and MAY set the Router option to the IP address of the DHCP proxy. It SHALL set the Domain Name Server option to the address of the DNS server contained in the NAS. Transaction ID is copied from the DHCPDISCOVER message. The DHCP proxy SHOULD send a single DHCPOFFER message.

If a DHCP Decline message is received, the ASN MUST not establish an IP session and SHALL release any existing Layer 3 session associated with this DHCP transaction.

For the subsequent DHCPREQUEST with the assigned IPv4 address, the DHCP proxy SHALL respond back to the MS with DHCPACK. In the DHCPACK message the DHCP proxy SHOULD set the address lease time parameters (T1 and T2 correspond to RENEWING and REBINDING state timers in the MS) as follows as default setting:

- $T_1 = 0.5 * \text{Lease Time}$
- $T_2 = 0.875 * \text{Lease Time}$

However, these values are configurable based on local network policy for optimization of network resources.

In order to reduce frequent address renewal messages over the air, the Lease Time SHOULD be set as reasonably large value.

In order to avoid possibilities of address collision when the MS is assigned a private IP address, the DHCP proxy SHALL use an operator-configured public IP address as its own address. It SHALL use this public IP address as the server identifier and the source IP address in the DHCP messages sent to the MS.

#### 4.13.4.2.2 DHCP Relay requirements

The DHCP relay SHALL handle all DHCP messages sent by the MS to the broadcast IP address.

The DHCP relay MAY be configured with the DHCP server address during the MS authentication. The VAAA or HAAA server MAY send the address of the v-DHCP or h-DHCP server respectively in the RADIUS Access-Accept packet or Diameter WDEA command. The DHCP relay MAY use this address to relay the DHCP messages from the MS to the DHCP server.

Upon receiving a DHCPDISCOVER message from the MS, the DHCP relay SHOULD verify the “chaddr” field in the DHCP header or in the client-identifier option matches the MS MAC address saved in the MS session context. This is done to prevent MAC address spoofing by a rogue MS. The ASN SHALL use the GRE key ID of the GRE tunnel over which the DHCP message (Offer/Ack) was received to locate the MS context.

If the DHCP relay determines that the MS has included a MAC address in the chaddr field or in the client-identifier options that does not match with the known MAC address in the MS context, the DHCP relay MAY consider the following action:

- A rogue MS trying to spoof MAC address. In this case, the DHCP relay MAY inform the DPF to initiate data path teardown.

The DHCP relay MAY add the relay agent option to the original DHCP message and set the Subscriber-ID suboption to the Outer-Identity (as defined in 4.4.1.3.1) associated with MS. If there is a secure communication channel between the DHCP relay and the DHCP server, the relay and server MAY choose to omit the authentication suboption.

The messaging between the DHCP relay and DHCP server is transported between ASN and CSN.

If a DHCP Decline message is received, the DHCP Relay SHALL forward the message to the DHCP Server.

When DHCP relay receives the DHCPOFFER message from the DHCP server, it SHALL relay it to the MS. If the DHCP server included the authentication suboption in the relay agent option, the DHCP relay SHALL validate it before relaying the DHCPOFFER to the MS.

The DHCP relay behavior for handling DHCPREQUEST or DHCPDECLINE from the MS is same as in the case of DHCPDISCOVER.

When the DHCP relay receives the DHCPREQUEST message from the MS, it MAY add a relay agent option to the message containing a Subscriber-ID suboption set to the MS Outer-Identity. The DHCP relay SHALL relay the DHCPREQUEST message to the DHCP Server. When DHCP relay receives the DHCPACK message from the DHCP Server, it SHALL relay the DHCPACK message to the MS.

The DHCP relay SHALL intercept DHCP renewal messages and verify the content of the message as described for DHCPDISCOVER message. The DHCP relay MAY add a relay agent option containing a Subscriber-ID suboption set to the MS Outer-Identity. If interface between ASN and CSN where DHCP server is residing is not secured (e.g. by IPSec), the DHCP relay MAY add the relay agent authentication suboption to the message before relaying it to the DHCP server.

In the case when DHCP lease time expires, the DHCP relay (if relay agent option was set) SHALL initiate the process of disconnecting the MS from the network and the ASN SHALL release all the resources related to the MS.

#### **4.13.4.2.3 DHCP server requirements**

The DHCP server SHALL support the procedures defined in RFC 2131, RFC 2132, RFC 3046 and RFC 3993.

The DHCP server SHALL be located in the VCSN or HCSN. The VAAA or HAAA server MAY assign a v-DHCP or h-DHCP server respectively for the MS during access authentication phase.

During the initial address assignment and the subsequent address renewals, the DHCP server receives DHCP messages from the DHCP relay in the ASN. If the message received by the DHCP server includes the relay agent authentication suboption, the DHCP server SHALL validate it and also include the relay agent authentication suboption in its response, so that DHCP relay can do the same. If the message received by the DHCP server includes the Subscriber-ID suboption in the relay agent option, the DHCP server may use the NAI from the Subscriber-ID as the identifier of the host instead of the chaddr field. The DHCP server SHALL process the DHCPDISCOVER and DHCPREQUEST messages sent by the relay agent and the DHCP Client according to RFC 2131 and RFC 3046.

Address assigned by the DHCP server SHALL be topologically anchored at the CR.

In the case when DHCP lease time expires, the DHCP server SHALL release any resources related to the MS.

#### **4.13.5 Requirements specific to Simple IPv6 service**

This section specifies additional requirements that are specific to Simple IPv6 service.

The IP link model for simple IPv6 service is based on the unique prefix per MS, in accordance with WiMAX Rel 1.0.

##### **4.13.5.1 MS Requirements**

There are no specific requirements on the IPv6 MS related to the simple IPv6 service. MS SHALL use either stateless (RFC 4862) or stateful (RFC 3315) address configuration mechanisms. Available address configuration

mechanisms are subject to the local network policy and the MS is informed about available methods via Router Advertisement message as per RFC 4861 and RFC 4862.

MS MAY use stateless DHCPv6 as per RFC 3736 to learn other network configuration information.

#### **4.13.5.2 DHCPv6 Requirements**

There are two different DHCP deployment modes possible:

DHCP proxy is in the ASN-GW.

DHCP relay in the ASN ASN-GW. DHCP server is located in the CSN

##### **4.13.5.2.1 DHCPv6 proxy requirements**

DHCP proxy SHALL support procedures defined in RFC 3315 and MAY support procedures defined in RFC 3736.

The address assigned to the MS SHALL be based on the prefix received by the NAS. If prefix information from both VCSN and HCSN are available, then there needs to be an anchor selection mechanism executed to select the anchor CSN for the data path. The details of this mechanism are outside the scope of this specification. If both prefix and interface-Id values are available to the NAS for the selected anchor CSN, then the DHCP proxy SHALL respond back to the MS setting the IPv6 Address field in the IA option to the address generated from the combination of the prefix and the interface id. If the Framed-Interface-Id or Visited-Framed-Interface-Id attribute is not present, then the DHCP proxy can pick a random interface id for generating the address.

When DHCP proxy detects that the lease time of an MS address has expired, it SHALL initiate procedures to tear down the MS IP session(s) using the expired address(es) and SHALL release any associated resources in the ASN.

If DHCP Release or DHCP Decline messages are received, the ASN SHALL release any existing Layer 3 session associated with this DHCP transaction.

##### **4.13.5.2.2 DHCPv6 relay requirements**

DHCP relay SHALL support procedures defined in RFC 3315.

DHCP relay SHALL relay all DHCPv6 messages received from the MS to the designated v-DHCPv6 or h-DHCPv6 server in the VCSN or HCSN respectively. The DHCP relay MAY be preconfigured with the address of the DHCP server or it MAY be provided with the DHCP server IP address by the VAAA or HAAA server in the RADIUS Access-Accept packet or Diameter WDEA command. The DHCP relay MAY be preconfigured with several DHCP server addresses and each of those DHCP servers may be accompanied by a domain name of the corresponding CSN operator. The DHCP relay MAY compare the domain part of the MS NAI with the domain name of the CSN operator and relay the DHCP messages to the DHCP servers matching the domain of the MS.

The messaging between the DHCP relay and the DHCP server is transported between ASN and CSN.

The DHCP relay MAY support procedures defined in RFC 4580. In this case the DHCP relay SHALL set the Subscriber-ID option to the Outer-Identity of the MS.

The DHCP relay MAY detect that the lease time of an address(es) assigned to the MS has expired. In such case DHCP relay SHALL initiate procedures to tear down the MS IP session(s) using the expired address(es) and SHALL release any associated resources in the ASN.

If Release or Decline messages are received by the DHCP relay, the ASN SHALL release any existing Layer 3 session associated with this DHCP transaction.

Messages between the DHCP relay and the DHCP server SHALL be exchanged securely.

##### **4.13.5.2.3 DHCPv6 server requirements**

DHCP server SHALL support procedures defined in RFC 3315 and MAY support procedures defined in RFC 3736 and RFC 4580.

A DHCP server SHALL be located in the VCSN or HCSN. The AAA server(s) (VAAA or HAAA) MAY assign a v-DHCP or h-DHCP server respectively for the MS during the MS access authentication phase. The DHCP server SHALL be located in the same CSN as the CR.

Address assigned by the DHCP server SHALL be topologically anchored at the CR. When choosing an address for the MS, the DHCP server MUST assign an address whose prefix is unique per MS, as per NWG Rel 1.0 IPv6 link model.

Messages between DHCP relay and DHCP server SHALL be exchanged securely.

#### **4.13.5.3 AR Requirements**

If the AR is configured to enable stateless address autoconfiguration of the MS address, it SHALL include the MS prefix in a Prefix Information Option of the Router Advertisement message. The 'A' flag in Prefix Information Option SHALL be set to true.

'L' flag in the Prefix Information Option SHALL be always false.

If the lifetime of the delegated prefix expires, the ASN SHALL release any existing Layer 3 session associated of all MSs whose address is based on the expired prefix.

The AR may be either preconfigured with a prefix pool from which it selects a prefix to be assigned to the MS or it MAY have received prefix from the AAA server in the Framed-IPv6-Prefix attribute.

#### **4.13.5.4 CR Requirements**

None.

### **4.14 Simple Ethernet Service Management**

This section describes procedures between the MS, ASN and CSN related to establishment and management of MS Ethernet connectivity in the Simple Ethernet mode.

During access authentication procedure ASN, V-CSN (if present) and H-CSN SHALL exchange their network service capabilities and negotiate the type of network service to be provided to the MS. Depending on the outcome of service negotiation process, Simple Ethernet service may be setup after successful access authentication. If more than one Ethernet service is authorized, the provided Ethernet service is based on local ASN policies.

The user plane traffic of simple Ethernet between the ASN and the CSN SHALL be delivered over existing data path. The exact type of the data path and mechanism used for path establishment are not defined by this specification. It is expected that the data path is established and maintained as per bilateral agreements between the WiMAX operators.

In the roaming case simple Ethernet service can either be provided by the visited CSN or by the home CSN of the MS. The selection of the designated CSN providing the simple Ethernet service in such case is subject to the agreements between operators. There must be a simple Ethernet data path between ASN and the CSN, which is providing the Ethernet services. In case of roaming with split ASN and CSN and Ethernet services provided by the H-CSN, the Simple Ethernet data path must traverse the V-CSN.

#### **4.14.1 MS requirement**

The MS providing ethernet services SHALL support Ethernet CS.

#### **4.14.2 L2 Forwarder (L2FW) requirements**

L2 Forwarder (L2FW) forwards user payload Ethernet frames in the upstream direction from R4/R6 datapath to R3 datapath and in the downstream direction from the R3 datapath to the R4/R6 datapath. It is equivalent to the AR in the IP Services case. The L2FW functionality is located in the ASN GW.

L2FW SHALL have a data path with the eCB in the CSN. L2FW MAY have several data paths for simple Ethernet service and each of these data paths SHALL be terminated by a different CSN, which MAY be owned by a different operator.

L2FW SHALL deliver all uplink traffic from the Ethernet MS to the CSN via the data path identifier contained in the MS context.

L2FW SHALL receive downlink MS traffic from the CSN via a data path. L2FW SHALL use data path identifier of the downlink packet to locate the MS context. If no matching MS context is found, the L2FW SHALL discard the received downlink packet.

While in active mode, the L2FW function handling the MS traffic can not be relocated for the duration of the MS MAC session.

#### **4.14.3 Ethernet Service Core Bridge (eCB) requirements**

Ethernet Service Core Bridge (eCB) is a bridge functional entity located in the CSN that terminates the simple Ethernet data path from the ASN. The eCB is a topological anchor for the MS Ethernet Service. It intercepts packets destined for the MS and delivers them to the ASN where the MS is located.

eCB SHALL have a data path with the L2FW. The eCB MAY have several data paths for simple Ethernet service and each of those data paths MAY be terminated by a different ASN owned by a different operator.

eCB SHALL deliver all downlink traffic for the simple Ethernet MS to the ASN where the MS is attached via the data path.

eCB SHALL receive uplink MS traffic from the ASN where the MS is attached via the data path.

#### **4.14.4 AAA server requirements**

AAA server SHALL authorize specific Ethernet service(s) and provide configuration information as a result of matching the ASN/CSN Ethernet service capabilities, the subscriber profile and the network policy. In case of successful access authentication, the RADIUS Access-Accept packet or Diameter WDEA command SHALL carry authorized Ethernet service information, configuration parameters corresponding to the authorized Ethernet service (anchored either in HCSN or VCSN).

#### **4.14.5 Layer 2 DHCP Relay requirements**

The layer 2 DHCP relay function SHALL be compliant with RFC 3046 and [15].

If the Authorized Network Services attribute in the final RADIUS Access-Accept packet or Diameter WDEA command indicates Layer 2 DHCP Relay service, then the ASN SHALL provide the layer 2 DHCP relay service for the MS being authenticated. In this case the ASN SHALL NOT provide the layer 3 DHCP relay service for this MS.

The L2 DHCP relay SHALL intercept all DHCP messages sent by the MS irrespective of whether the messages are sent to the broadcast or unicast address.

The DHCP relay SHALL add the relay agent option to every intercepted message before relaying it towards the core network. Following suboptions SHALL be added as part of the relay agent option and they SHALL be initialized as follows:

Remote ID suboption SHALL be set to the MS-ID. MS-ID SHALL NOT be copied from the chaddr field of the DHCP message but it SHALL be taken from the MS context. The MS context is located by using the GRE key of the GRE tunnel over which the DHCP message is received.

Circuit ID suboption SHALL be set to the BS-ID identifying the base station to which the DHCP response message SHALL be delivered towards the MS.

Subscriber ID SHALL be set to the Outer-Identity of the MS.

WiMAX Radio Link Characteristics vendor specific suboption MAY be included and MAY contain any suboption defined in section 5.6.1.

DHCP relay SHALL intercept every downlink DHCP message and remove the relay agent option before delivering the message towards the MS. The DHCP relay SHALL use the Circuit ID suboption to identify the BS to which the message SHALL be delivered.

DHCP relay SHALL silently discard any DHCP OFFER and DHCP ACK messages that are sent by the MS. DHCP relay MAY log such an event.



In the case when DHCP lease time expires, the DHCP relay SHALL initiate the process of disconnecting the MS from the network and the ASN SHALL release all the resources related to the MS.

## 4.15 Release and Capability Negotiation Function on R4/R6/R8

### 4.15.1 General

This section specifies a procedure for negotiation of the WiMAX release and the optional capabilities to be applied between network components in the NAP (among BSs and ASN GWs) across reference points R6 and R4 as well as R8 if available. The procedure aims at guaranteeing the interoperability between network nodes, in spite of the existence of more than one WiMAX Release (currently R1.0 and R1.5) and in spite of several features and capabilities being optional. The procedure may help to simplify the network node configuration since it allows for the network nodes to inform each other about their capabilities such that this knowledge about the capabilities of neighbor nodes will be available in each node whenever required, and does not necessarily have to be configured.

The procedure can be applied in the absence of neighbor node knowledge configuration, or in addition to such configuration.

The procedure is based on the following considerations:

- Network Nodes in the NAP network need to communicate with other network nodes in the NAP network.
- The communication needs to be based on an agreement on the same WiMAX Release to be used at both sides.
- The communication between two nodes A and Z, being based on release R<sub>i</sub>, may involve certain capabilities C<sub>j</sub>.
- For proper application of such capability C<sub>j</sub>, it may be necessary that the initiating node, say node A, can be sure that the communication peer, say node Z, supports this capability.
- Therefore each node, say node A, might have a database that indicates, for each WiMAX release that node A supports, and for each capability C<sub>j</sub> that node A wishes to use under this release, and for each neighbor node Z that may be a communication peer for this capability, whether node Z supports this capability.
- The procedure provides means for node A to ask the suitable “capability request” question to any applicable node Z, in order to get a response from node Z and by that to learn about Z’s capability support and to fill or maintain the capability database in node A. This can be considered a “pull” procedure.
- In addition, the same procedure should allow to agree on the common release and the common capability set to use between two nodes A and Z, in case the set of commonly supported releases and capabilities would allow more than one choice to agree on.
- In addition to the “pull” procedure, there are situations where a “push” procedure may be required to keep the capability database in a node A up to date when the capabilities in a neighbor node Z vary. The capability variation may be an upgrade, e.g. support of new capabilities of even a new release – or a downgrade. In this case, node Z should automatically inform node A that node A should update its neighbor node capability database for consistency. This can be considered a “push” procedure.
- In order for node Z to recognize the need for initiating a “push” procedure with node A, each node Z should be aware of which capabilities it has committed to node A, such that node Z can decide which of its neighbor nodes A need to be informed about a new, modified or deleted capability of node Z.
- While the details of any potentially existing neighbor node capability database in the network nodes are not subject to standardization, the procedure specified below is based on some basic assumptions on the database in each involved node, as outlined above.

In the following, the procedure is introduced as a stand-alone procedure, which can be applied at any time, independent from other ASN control procedures.

Negotiating the capability of network nodes may also be done based on information that is piggy-backed to existing procedures, e.g. in case of the ROHC capability, the “ASN-GW ROHC Capability” TLV is carried in the Anchor\_DPF\_HO\_Trigger. The piggybacked method and the stand-alone procedures may complement each other, and the piggybacked method might be extended to cover more capabilities (left for further study). The nodes may use any of the methods dynamically to indicate the current feature support/non support state.

#### 4.15.2 Procedure Specification

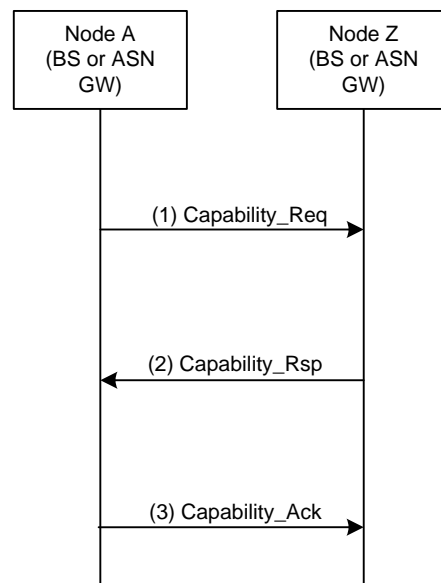
The procedure includes three messages to be used as a 3-way handshake:

- 1) Capability\_Req
- 2) Capability\_Rsp
- 3) Capability\_Ack

The procedure may be executed between any two network nodes, say node A and node Z, for updating each other’s knowledge about their supported releases and/or capabilities. Such node A or node Z can be a Base Station or an ASN GW:

- If applied on R6, one node is a BS and the other is an ASN GW
- if applied on R4, both nodes are an ASN GW
- If applied on R8, both nodes are a BS.

The procedure is applicable between any two nodes that may be originator and terminator of a WiMAX Control procedure – which may also include the case where an ASN GW serving as Relay node is relaying the capability negotiation messages. An ASN GW serving as relay of capability negotiation messages SHALL be transparent for the message content (by definition of the relay function), so the release and capabilities of such Relay ASN GW SHALL be out of scope for capability negotiation between the two signaling endpoints which may be two Base Stations using R6 and ASN GW Relay for inter-BS communication. In the following diagram, such potentially present Relay node is not shown, for simplicity.



**Figure 4-185 – Release/Capability negotiation procedure (push or pull mode)**

The procedure steps are as follows:

## STEP 1

Once Node A has recognized the need for performing the release/capability negotiation procedure with another network node, say Node Z, it may send the Capability\_Req message to Node Z.

Examples of triggers for starting the procedure may be the following:

- Node A wishes to communicate to Node Z and needs to agree on the Release (R1.0 or R1.5). This may involve both “push” and “pull” aspects, i.e. information exchange in both directions.
- Node A wishes to execute a function with Node Z where support of capability  $C_j$  by Node Z is required, and Node A does not have local knowledge yet about Z’s support of capability  $C_j$ . This is a case for the “pull” method.
- Node A has been upgraded such that it supports capability  $C_j$  which it previously did not support. Node A remembers that Node Z had asked for this capability earlier, and Node A had denied capability  $C_j$  before. So Node A decides to update Node Z about the upgrade. This is a case of “push” procedure.

There is no need for Node A to include ALL its supported releases and ALL its supported capabilities in the Capability\_Req message. So from the absence of a certain capability identifier in the Capability\_Req message, node Z SHALL NOT conclude that this capability is not supported by A. – If node Z wishes to check the support of capability  $C_j$  by node A, and Z does not see this capability in a Capability\_Req message received from node A, then node Z may initiate its own capability negotiation procedure at a later point in time as a “pull” procedure, by sending a Capability\_Req message to node A, asking for the specific capability.

So Node A sends the Capability\_Req message to Node Z, including one or more release indicators and for each release, those capabilities that A supports and which A wants Z to become aware of, or those capabilities that A supports and where A wishes to learn whether Z supports them as well, or both kinds of capabilities.

## STEP 2

Upon reception of the Capability\_Req message, node Z performs the following:

- Z compares the release indication included in the received message, and compares it to its own supported releases. If Z sees it can support the highest release out of the releases in the Capability\_Req message, it will report this release back in the Capability\_Rsp. Otherwise, Z should report its own highest supported release – offering to A to continue with this lower release number.
- Z also checks the list of capabilities in the Capability\_Req message and checks which of them it supports; in the Capability\_Rsp message, it SHALL indicate the level of support (in most cases just Yes/No) for these capabilities. If Z does not understand a certain capability identifier in the Capability\_Req message, it should just ignore it and not include that identifier in the Capability\_Rsp message. From the absence of a response to such capability identifier in the Capability\_Rsp message, node A will learn that node Z does not support this capability.
- There is no need for node Z to list all its own releases or capabilities in the Capability\_Rsp message; node Z is only mandated to give a complete answer to the releases and capabilities listed in the Capability\_Req message. So when node A receives the Capability\_Rsp message, it can be sure about the support of those releases and capabilities by node Z but node A cannot conclude about any other capabilities which are neither listed on the Capability\_Req nor in the Capability\_Rsp.

Then Z should send the suitably equipped Capability\_Rsp message back to node A.

## STEP 3

Upon receiving the Capability\_Rsp message, node A SHALL send back a final Capability\_Ack message, confirming the agreed release.

The Capability\_Ack message may also be used to reject the Release or capability proposal offered by node Z in the Capability\_Rsp message – in particular if node Z is not able to support the release and capabilities requested by node A, and offered a downgraded alternative only. In this case, Node A may decide to stop communicating with that node, due to release or capabilities incompatibility.

Note that the layout of these three messages allow to perform a “lightweight” version of the capability negotiation procedure, e.g. by indicating a release exchange only without listing any capabilities; as said above, the absence of capabilities in the Capability\_Req message does not mean that node A does not support these; Node Z should in this case just keep the status of the not mentioned capabilities of Node A unchanged.

### 4.15.3 Message definitions

As said above, the release and capabilities procedure is based on three messages which are specified here: 1) Capability\_Req, 2) Capability\_Rsp, 3) Capability\_Ack.

**Table 4-190 – Capability\_Req**

IE	Reference	M/O	Notes
WiMAX Release Info (one or more)	5.3.2.426	M	At least one WiMAX_Release_Info TLV SHALL be included.
>R4R6R8WiMAX Release	5.3.2.427	M	Each WiMAX_Release_Info TLV SHALL include the WiMAX_Release it refers to.
>Capabilities Info	5.3.2.428	O	List of capabilities which are supported by the sending node for the indicated WiMAX_Release. The Capabilities_Info_TLV SHALL be omitted if the list is empty.
Capabilities Negotiation Mode	5.3.2.229	O	Indicates the Capabilities Negotiation Mode. The value may be set to: 1 – Complete List of Capabilities 2 – Individual Capabilities
>>ASN-GW ROHC Capability	7.3.2.7 of the ROHC Standalone Spec	O	To indicate whether ROHC is supported or not supported. An entry with the value “not supported” SHALL be inserted if the capability had been present previously and has been deleted.
>>Support-of-MCBCS	5.3.2.429	O	To indicate whether MCBCS is supported or not.
>>Support-of-HO-DI	5.3.2.430	O	To indicate whether HO-DI is supported or not.
>>Support-of-dMAC	5.3.2.431	O	To indicate whether dMAC is supported or not.
>>Support-of-Accounting	5.3.2.432	O	Indicates which accounting modes are supported.
>>Support-of-IMS-ES	5.3.2.433	O	To indicate whether IMS-ES is supported or not.
>>Support-of-PCC-QoS	5.3.2.434	O	To indicate whether PCC-QoS is supported or not.
>>Support-of-EtherServ	5.3.2.435	O	To indicate whether EtherServ is supported or not.
>>Support-of-LBS	5.3.2.436	O	To indicate whether LBS is supported or not.
>>Support-of-FixedNom	5.3.2.437	O	To indicate whether FixedNom is supported or not.
>>Support-of-Hotlining	5.3.2.438	O	Indicates which Hot-Lining modes are supported.
>>Support-of-RRM	5.3.2.439	O	To indicate whether RRM is supported or not.

This message is sent from a network node (say “Node A”, i.e. a BS or an ASN GW) to another network node (say “Node Z”), for the purpose of informing Node Z about the selected subset of releases and capabilities, and to request

a response from Z on whether Z supports these releases and capabilities. Absence of a capability in the Capabilities list does not mean the capability is not supported.

The sending node (Node A) is identified by the Source IP address of the message (in case of no relay function being involved) – or by the Source ID TLV in case of message relay. The receiving node (Node Z) is identified by the Destination IP address (in case of no relay function being involved) – or by the Destination ID TLV in case of message relay.

**Table 4-191 – Capability\_Rsp**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
WiMAX Release Info (one or more)	5.3.2.426	M	The Releases addressed in this message SHALL be a copy or a subset of the list of Releases in the Capability_Req message. At least one WiMAX_Release_Info TLV SHALL be included. If a WiMAX_Release_Info TLV is included, it means the sender of Capability_Rsp supports that release.
>R4R6R8 WiMAX Release	5.3.2.427	M	Each WiMAX_Release_Info TLV SHALL include the WiMAX_Release it refers to.
>Capabilities Info	5.3.2.428	O	This list SHALL be a copy or subset of the capabilities list in the Capability_Req message, and SHALL indicate which of the capabilities listed in the Capability_Req messages are also supported by the receiver of that message. If any of the capabilities had been present in the Capability_Req message and is not included in the Rsp, it means the capability is not supported by the sender of the Rsp message.
Capabilities Negotiation Mode	5.3.2.229	O	Indicates the Capabilities Negotiation Mode. The value may be set to: 1 – Complete List of Capabilities 2 – Individual Capabilities
>>ASN-GW ROHC Capability	7.3.2.7 of the ROHC Standalone Spec	O	To indicate whether ROHC is supported or not.
>>Support-of-MCBCS	5.3.2.429	O	To indicate whether MCBCS is supported or not.
>>Support-of-HO-DI	5.3.2.430	O	To indicate whether HO-DI is supported or not.
>>Support-of-dMAC	5.3.2.431	O	To indicate whether dMAC is supported or not.
>>Support-of-Accounting	5.3.2.432	O	Indicates which accounting modes are supported.
>>Support-of-IMS-ES	5.3.2.433	O	To indicate whether IMS-ES is supported or not.
>>Support-of-PCC-QoS	5.3.2.434	O	To indicate whether PCC-QoS is supported or not.
>>Support-of-EtherServ	5.3.2.435	O	To indicate whether EtherServ is supported or not.
>>Support-of-LBS	5.3.2.436	O	To indicate whether LBS is supported or not.

IE	Reference	M/O	Notes
>>Support-of-FixedNom	5.3.2.437	O	To indicate whether FixedNom is supported or not.
>>Support-of-Hotlining	5.3.2.438	O	Indicates which Hot-Lining modes are supported.
>>Support-of-RRM	5.3.2.439	O	To indicate whether RRM is supported or not.

This message is sent from a network node (say “Node Z”, i.e. a BS or an ASN GW) to another network node (say “Node A”), in response to a Capability\_Req message, for the purpose of informing Node A about the support of the selected subset of releases and capabilities by Node Z. An absence of a capability in Capability\_Rsp message, that had been present in the Capability\_Req message, means that this capability is not supported by Node Z.

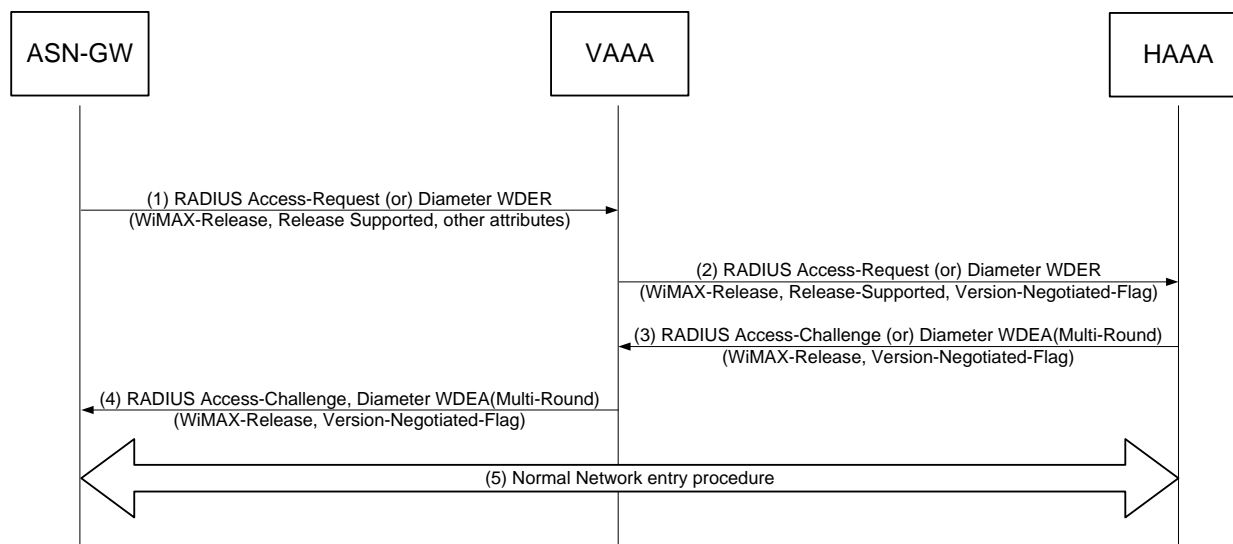
The sending node (Node Z) is identified by the Source IP address of the message (in case of no relay function being involved) – or by the Source ID TLV in case of message relay. The receiving node (Node A) is identified by the Destination IP address (in case of no relay function being involved) – or by the Destination ID TLV in case of message relay.

**Table 4-192 – Capability\_Ack**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
R4R6R8 WiMAX Release Info	5.3.2.426	O	The ACK message SHALL indicate the common, agreed Release. – If Node A does not agree to any of the releases offered by Node Z, the WiMAX_Release_Info TLV SHALL be omitted, which means there is no basis for further signaling between the involved nodes.
>WiMAX Release	5.3.2.427	CM	To be included if the parent TLV is present.

## 4.16 R3-R5 Version Negotiation

This section describes version negotiation whereby the NAS (ASN-GW or HA) and the Home AAA (as well as the VAAA) negotiate a common protocol for AAA (R3/R5). The following call flow illustrates the Version Negotiation procedure.



**Figure 4-186 – Network Entry with R3-R5 Version Negotiation Procedure**

### STEP 1

During an MS's Network Access Authentication and Authorization as described in section 4.4.1, the NAS selects a version to communicate with the Home CSN. The version selected is either pre-configured, previously negotiated, or based on local-policies. The NAS codes the AAA message (RADIUS Access-Request, Diameter WDER) using the version selected and sets the WiMAX-Release TLV of the WiMAX-Capability attribute to the version selected. In addition, the NAS sets Release-Supported TLV to a comma-separated list of supported WiMAX releases.

### STEP 2

When the VAAA receives the AAA message for this new session, if it does not support the version proposed by the NAS, it may suggest its own version by selecting a version that it supports from the list proposed by the NAS in the Release-Supported TLV of the WiMAX-Capability attribute. The VAAA sets the WiMAX-Release TLV of the WiMAX-Capability attribute to the value of the version it selected. The VAAA removes all undesired version proposed by the NAS from the Release-Supported TLV of the WiMAX-Capability attribute. The VAAA adds the Version-Negotiation-Flag set to TRUE in the WiMAX-Capability attribute to indicate that the AAA request message is to be used only for version negotiation.

### STEP 3

When the HAAA receives the AAA message for this new session, if it supports the version stated in the WiMAX-Release TLV of the WiMAX-Capability attribute and the WiMAX-Capability attribute does not contain the Version-Negotiation-Flag set to TRUE, then it proceeds as usual with the authentication procedure of this session. From this point on, the negotiated version will be used for this session.

If however the WiMAX –Capability attribute contains the Version-Negotiation-Flag set to TRUE or if the HAAA does not support the proposed version, then the HAAA responds with an Access-Challenge AAA message (RAIDUS Access-Challenge Diameter WDEA(Multi-round)) which includes no authorization attributes or an EAP-Message. In the case where the HAAA does not support the proposed version in the WiMAX-Release TLV of the WiMAX-Capability attribute, the HAAA selects a version that it supports from the Supported-Release TLV of the WiMAX-Capability attribute. The HAAA sets the WiMAX-Release TLV of the WiMAX-Capability attribute to the release it selected and includes the Version-Negotiation-Flag TLV set to TRUE in the WiMAX-Capability attribute. In either case the HAAA does not include the WiMAX-Capability Release-Supported TLV.

**STEP 4**

The VAAA receives the AAA-Challenge message and passes it to the NAS. The VAAA records the version contained in the WiMAX-Release TLV of the WiMAX-Capability attribute as the version to be used for this session.

**STEP 5**

The NAS receives the AAA Challenge message.

If the Version-Negotiation-Flag TLV is not included in the WiMAX-Capability attribute and the WiMAX-Release TLV of the WiMAX-Capability attribute contains the same release proposed by NAS, then the NAS will continue performing the authentication procedure for that session.

If the Version-Negotiation-Flag TLV is included in the WiMAX-Capability attribute and the WiMAX-Release TLV of the WiMAX-Capability attribute contains a different release than the one proposed by the NAS, then the NAS re-issues the Access-Request encoded using the value specified in the WiMAX-Release TLV. The NAS will use that proposed release for the lifetime of the session.

To avoid constant R3/R5 version negotiation, the NAS may cache the negotiated version against the home realm. If the NAS employs a caching strategy and if the negotiated version was not the same as the NAS initially proposed, then the NAS could periodically re-try to negotiate its preferred version.

**4.16.1 Version Alignment Between ASN-GW and HA**

The WiMAX Release is separately negotiated between the ASN-GW and the HAAA, and between the HA and the HAAA. Ideally the version negotiation should align especially when the HA is in the VN-SP. However, in cases when the negotiated versions do not align, it is expected that the Home AAA will cope with the differences.

**4.16.2 Requirements**

**4.16.2.1 General Requirements**

An ASN-GW, HA or HAAA that support this release SHALL use the string “1.5” as the version indicator for this release.

**4.16.2.2 NAS Requirements**

These requirements are applicable to the NAS (ASN-GW and the HA).

When performing initial network entry (in the case of ASN-GW) or initial authentication for Mobile IP (in the case of a HA) with a given HAAA (based on home realm), the NAS SHALL select the latest version of the R3/R5 protocol that it supports; or a previously negotiated version, if the NAS cached a previous negotiated version.

The ASN-GW SHALL use the selected version to encode the RADIUS Access-Request message or Diameter WDER command; and the HA SHALL use the selected version to encode the RADIUS Access-Request message or Diameter WHAR command by setting the following:

- The NAS SHALL set the WiMAX-Release TLV of the WiMAX-Capability attribute to the version selected.
- The NAS SHALL set the Release-Supported attribute in the RADIUS Access-Request or Diameter WDER command to the versions of R3/R5 that it supports. If the NAS does not support any other releases it SHALL omit this attribute.
- The NAS SHALL NOT include the Version-Negotiation-Flag TLV in the WiMAX-Capability attribute.

Upon receiving a AAA response message (in the case of RADIUS Access-Challenge message, and in the case of Diameter WDER command with Diameter Multi-round indication) that contains a WiMAX-Capability attribute without the Version-Negotiation-Flag TLV and a WiMAX-Release TLV set to the same value set by the NAS in AAA request message, then the NAS SHALL continue the Network Entry Authentication procedure and use this version for the associated WiMAX session.



Upon receiving a response from the HAAA that contains a WiMAX-Capability attribute with the Version-Negotiation-Flag TLV set to the value three(3), and the WiMAX-Release TLV set to a version that is supported by the NAS, the NAS SHALL resend the original AAA request message coded according to the version specified by the WiMAX-Release TLV. If the WiMAX-Release TLV is set to a version that the NAS does not support, the NAS SHALL treat the AAA response as a rejection.

In the case of successful version negotiation, the NAS SHALL use that version for all subsequent interaction with the HAAA for that WiMAX Session. In addition, the NAS MAY cache this version to use for communicating with the home realm for other WiMAX sessions. In the case of using a previously negotiated version, the NAS SHOULD periodically try to renegotiate the latest version that it supports.

#### 4.16.2.3 VAAA Requirements

This section describes the requirements of a VAAA with respect to R3/R5 version negotiation.

When a VAAA receives an AAA message corresponding to an initial network entry procedure or initial MIP session authentication (WiMAX-Session-Id attribute is not included in the AAA message) it performs the following actions.

The VAAA MAY modify the Release-Supported TLV of the WiMAX-Capability attribute by removing any releases that it does not support.

If the VAAA agrees with the version proposed by the NAS in the WiMAX-Release TLV of the WiMAX-Capability attribute, it SHALL set the Version-Negotiation-Flag TLV of the WiMAX-Capability attribute to the value of one(1).

Otherwise, if the VAAA does not agree with the proposed value set by the NAS, it SHALL set the WiMAX-Release TLV of the WiMAX-Capability attribute to the highest version that it supports from the Release-Supported TLV of the WiMAX-Capability attribute, and set the Version-Negotiation-Flag TLV of the WiMAX-Capability attribute to the value of two(2).

If the VAAA does not agree with the proposed value set by the NAS, and it does not support any of the versions proposed in the Release-Supported TLV of the WiMAX-Capability attribute, then the VAAA SHALL send an Access-Reject AAA message with error indication that it does not support the version proposed. In the case of RADIUS, the Error-Cause attribute SHALL be set to “Invalid Request”(404). In the case of Diameter the Result-Code SHALL be set to “DIAMETER\_UNABLE\_TO\_COMPLY” (5012).

The VAAA SHALL NOT modify messages sent by the HAAA to the NAS in the process of version negotiation. If the version is negotiated for that session, the VAAA SHALL record this version.

#### 4.16.2.4 HAAA Requirements

When a HAAA receives an AAA message corresponding to an initial network entry procedure or initial MIP session authentication (WiMAX-Session-Id attribute is not included in the AAA message) it SHALL participate in R3/R5 version negotiation as described in this section.

If the WiMAX-Release TLV contained in the AAA request message:

- Is set to a release that the HAAA agrees to, and
- In the case of roaming (VAAA is present) the Version-Negotiation-Flag TLV is set to one (1); or
- In the case of non-roaming (VAAA is not present) the Version-Negotiation-Flag TLV is not present;

Then the HAAA SHALL proceed with the Initial Network Entry procedures or MIP Session Authentication procedures as described in this document. The negotiated release contained in the WiMAX-Release TLV SHALL be used for this WiMAX session.

If the WiMAX-Release TLV contained in the AAA request message:

- Is set to a release that the HAAA supports; and
- If the Version-Negotiation-Flag TLV is set to two(2);

Then the HAAA SHALL respond with an RADIUS Access-Challenge or Diameter WDEA command with indicating MULTI-ROUND, with Version-Negotiation-Flag TLV set to three (3) indicating that the AAA answer message is used for version negotiation.

1 If the HAAA does not support the release proposed in the WiMAX-Release TLV of the WiMAX-Capability  
2 attribute, then the HAAA SHALL set the WiMAX-Release TLV of the WiMAX-Capability attribute to the highest  
3 supported release in the Supported-Release TLV of the WiMAX-Capability attribute that it prefers to use. In this  
4 case it SHALL set the Version-Negotiation-Flag TLV to three (3) indicating that the AAA Answer message is used  
5 for version negotiation.

6 If the HAAA does not support the proposed version in the WiMAX-Release TLV and the Supported-Release TLV  
7 does not contain a release agreeable to by the HAAA, then the HAAA SHALL respond with an AAA Rejection  
8 message (in the case of RADIUS Access-Reject packet and in the case of Diameter, WDEA or WHAA with result-  
9 code set to indicate failure). The AAA message SHALL indicate the cause of the error by:

- 10 • In the case of RADIUS the Error-Cause attribute SHALL be set to “Invalid-Request”(404); and
- 11 • In the case of Diameter the Result-Code SHALL be set to “DIAMETER\_UNABLE\_TO\_COMPLY”  
12 (5012).

### 13 4.16.3 Support for Release 1.0 VAAA

14 The HAAA is required to detect the presence of a VAAA. The HAAA uses the presence of the NSP-ID set to a  
15 different identity than the H-NSP to detect roaming and hence the presence of a VAAA.

16 In the case of roaming – the HAAA detects the presence of a VAAA - if the Version-Negotiation flag is not present  
17 and the WiMAX-Release TLV is not specifying Release 1.0 then the HAAA SHALL negotiation Release 1.0 by  
18 setting WiMAX-Release to 1.0 and setting the Version-Negotiation flag to three(3).

19 The VAAA that complies with release 1.5 is required to add attributes such as the Version-Negotiation-Flag TLV  
20 that appears in the WiMAX-Capability attribute.

21 The VAAA that is compliant with release 1.0 is not required to insert a Version-Negotiation-Flag TLV but is  
22 required to ensure an NSP-ID is present in the Access-Request set to the V-NSP identity. If this NSP-ID is not  
23 included by the NAS the VAAA SHALL insert this attribute in the Access-Request packet.

24 The HAAA uses the presence of an NSP-ID set to a different identity than the H-NSP to detect roaming and hence  
25 the presence of a VAAA.

## 26 4.17 Keep-alive mechanism

27 The following section describes Keep-alive mechanism between Network Entities (NE) in WiMAX Access Network  
28 associated to provide service for the same MS. This mechanism may be used over R6/ R4 reference points and  
29 provides each side with capability to detect failure/ restart of its peer. The NE, detecting the failure/ restart of the  
30 peer may take appropriate actions – e.g. clean up the corresponding MS contexts in a “controlled” way.

31 The Keep-alive mechanism is based on a 2-way transaction (*Keep-alive Req/ Rsp* message exchange). Every NE  
32 MAY perform its own independent keep-alive procedure. The trigger for sending *Keep-alive Req* message is out of  
33 the specification scope. As an example of one implementation, NE may trigger *Keep-alive Req* to the peer node at  
34 the moment it shares MS context with that node. NE MAY continue sending *Keep-alive Req* messages periodically,  
35 as long as it shares any MS context with the peer node. Another example is that NE may trigger *Keep-alive Req* to  
36 the peer node at the moment it starts working right after it turns on.

37 A NE MAY trigger keep-alive transaction to its peer on a periodic basis thus:

- 38 • informing its aliveness to the peer and/ or requesting the sign of life from the peer;
- 39 • informing a self reboot event of the sending NE and/ or detecting the peer node reboot events since the last  
40 keep-alive interrogation.

41 The NE that supports keep-alive functionality, at the moment of its boot up, SHALL generate the non-zero 32-bit  
42 (UTC) timestamp (Last Reset Time) and cache it internally. The NE SHOULD ensure that this value is unique  
43 across the multiple restarts of the NE. When sending *Keep-alive Req or Rsp* message, the NE SHALL include this  
44 LRT value in the message. This value MAY be interpreted by the keep-alive Receiver to detect the peer's restart  
45 (when it detects that the received value does not match the one previously advertised by the NE).

If the restart preserves the MS contexts which was stored before the reboot, the NE SHALL NOT change its LRT value after the reboot. Otherwise, NE SHOULD change its LRT value after the reboot in order to inform the peer node of its reboot.

The Receiver of keep-alive message MAY interpret Last Reset Time TLV value as a Timestamp (UTC), or 32-bit unique value. Interpreting LRT value as a Timestamp allows recovery optimization, - such as selective clean-up of MS contexts in the case of peer node restart detection (based on NE knowledge of the MS context creation time).

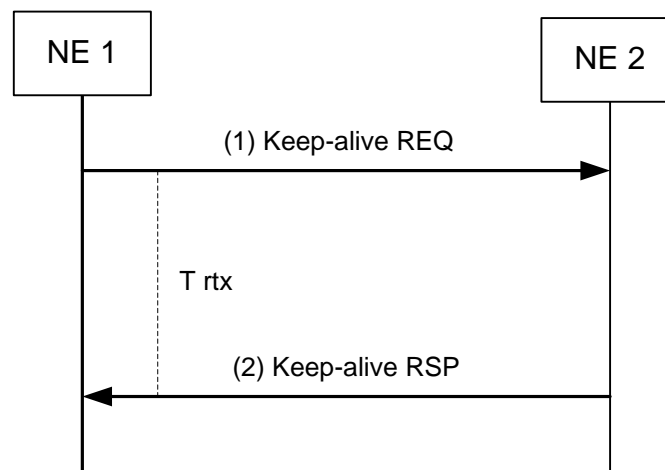
The mechanism for detection of the peer node restart is as following:

- The NE SHOULD store the LRT value of its peer nodes as received in the initial keep-alive interrogation with the particular peer.
- In any subsequent keep-alive interrogation, the NE SHALL compare the received LRT value with the stored non-zero value. If the received LRT value does not match the stored non-zero value for the peer node, the NE SHALL consider the peer node has passed restart during the time interval from the last keep-alive interrogation and MAY take an appropriate action. The action may be implementation-specific (e.g. purge out the corresponding MS contexts, trigger MS Network Exit for the impacted MSs, etc.)
- The NE that detects the peer node restart SHALL store the new LRT value for this peer node.
- As an optimization, the NE, that interprets the received LRT value as a Timestamp, MAY be able to perform selective MS context clean-up, based on its knowledge of MS context creation time.

This specification does not define any optimization for the message load. For example, in full mesh and very frequent keep alive exchanges, the load at some NEs should be considered. One way to prevent full mesh exchanges is to use optional “health status” reporting on behalf of other node(s); other options include a configuration of infrequent keep alive messages (with a side effect of slower failure detection) or a controlled selection of keep alive peers.

Keep-alive functionality may be further extended to support failure event reporting on behalf of the peer node (thus reducing the Keep-alive messaging load).

The following call flow presents the keep-alive procedure.



**Figure 4-187 – Keep-alive procedure**

#### STEP 1

The NE1 triggers keep-alive interrogation with NE2 by sending *Keep-alive Req* message. This message SHALL include Last Reset Time TLV and MAY include Health Status TLV.

**Table 4-193 – Keep-alive Req**

IE	Reference	M/O	Notes
Last Reset Time	5.3.2.442	M	The timestamp of the Keep-alive REQ Sender's last boot up (the value generated during the NE last boot up).
Health status	5.3.2.443	O	Zero or more TLVs MAY be included.
> Status	5.3.2.444	CM	SHALL be included if Health Status TLV is included. It provides the reported NE/ Function status (as identified by Functional Entity ID of the Reported Node if present, or by originator of the message if Reported Node ID is not present).
> Reported Node ID	5.3.2.445	O	MAY be included if the report is on behalf of another reported Node. Identifies the Functional Entity ID (the addressable ID which can be presented by IPv4, IPv6 or IEEE 6-octet address) of the reported node.
> Reference Last Reset Time	5.3.2.446	O	SHALL be included if Reported Node ID TLV is included. Provides the LRT value of the reported NE (as identified by Functional Entity ID of the reported node).
> Function ID	5.3.2.447	O	MAY be included to indicate the specific WiMAX ASN GW Functional Entity as defined for WiMAX ASN GW – Authenticator, Anchor GW or PC. If missing, the Default value (ALL) is assumed.

The NE2 receiving *Keep-alive Req* from NE1 MAY recognize that NE1 is “alive” and MAY compare the received LRT value with the stored non-zero value for NE1 (as received from previous keep-alive interrogations). If the received LRT value does not match the stored non-zero value for the peer node, the NE2 considers the peer node has passed a restart during the time interval from the last keep-alive interrogation. In this case NE2 MAY take an appropriate action (e.g. purge out the corresponding MS contexts).

If this is the first keep-alive interrogation from NE1, NE2 MAY store the received LRT value against NE1 identity.

The NE2 receiving *Keep-alive Req* with included Reported Node ID TLV (in Health Status TLV), MAY recognize the referred NE or function (if Function ID is also included) health state specified by the Status TLV. It MAY take an appropriate action depending on the actual status. For instance, NE2 MAY terminate all MS sessions and corresponding data paths for MSs belonging to the referred NE when the reported status is FAILED or SHUTTING DOWN. It also MAY compare the included Reference LRT to the stored previously known non-zero LRT for the same NE. If the received Reference LRT value does not match the stored previously known non-zero LRT, NE2 considers that the referred NE or function has passed through at least a single restart since the last keep-alive exchange. In this case NE2 may take an appropriate action.

NE2 receiving *Keep-alive Req* with Status TLV, but without Reported Node ID TLV (in Health Status TLV) MAY recognize the state of the peer NE (NE1 in the example) or function (if Function ID TLV is also included) as announced by the value of Status TLV. In such a case, the NE2 MAY take an appropriate action depending on the reported peer NE status.

## STEP 2

The NE2 responds back to the NE1 with *Keep-alive RSP* message and includes Last Reset Time TLV set to the last recorded time of the NE2 boot up.

**Table 4-194 – Keep-alive Rsp**

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
Last Reset Time	5.3.2.442	M	The timestamp of the Keep-alive RSP Sender's last boot up (the value generated during NE last boot up).

NE1 receiving *Keep-alive Rsp* message from NE2 MAY recognize that NE2 is “alive” and SHALL compare the received LRT value with the stored non-zero value for NE2 (as received from previous keep-alive interrogations). If the received LRT value does not match the stored non-zero value for the peer node, the NE1 considers the peer node has passed a restart during the time interval from the last keep-alive interrogation. Note that in this case NE1 may take an appropriate action, which is implementation specific.

If this is the first keep-alive interrogation to NE2, NE1 stores the received LRT value against NE2 identity. If the Failure Indication TLV is included in the message, the message may not include the Last Reset Time TLV.

### 4.17.1 Requirements

#### 4.17.1.1 Keep-alive Req Sender requirements

Support of keep-alive functionality is optional. The NE that supports keep-alive functionality MAY send *Keep-alive Req* message to its peers. The MSID field in the header of *Keep-alive REQ* message SHALL be set to all zero and the C-bit SHALL be set to 1 to require comprehension for the message.

The sender of the Keep-alive Req message SHALL always include Last Reset Time TLV with the value that was set right after the last boot-up in the Keep-alive Req messages.

The sender of the message expects to receive *Keep-alive Rsp* message within some time interval ( $T_{rx}$ ). If not received, the sender MAY perform retransmissions and if no response even for the retransmissions, MAY consider the peer NE as “unavailable” and take an appropriate action. The keep-alive retransmission mechanism and retransmission timer ( $T_{rx}$ ) are out of the specification scope.

The sender may receive “general error” indication as specified in the section 3.4 – means the peer node does not support keep-alive functionality. In this case, the sender SHOULD stop sending *Keep-alive Req* messages to this peer. The sender MAY re-try it later for various reasons.

When the sender receives *Keep-alive Rsp*, it SHALL check the LRT value received from the peer. If the LRT value received in Keep-alive Rsp does not match the stored non-zero value for the peer node, the sender SHALL consider the peer node has passed restart during the time interval from the last keep-alive interrogation. Note that the sender may take the appropriate action, which is implementation specific.

The sender that performs the first keep-alive interrogation to its peer, SHALL store the received LRT value against the peer's identity.

#### 4.17.1.2 Keep-alive Req Receiver requirements

NE that supports keep-alive functionality, SHALL respond back to the keep-alive originator with *Keep-alive Rsp* message on each *Keep-alive Req* message it receives, no matter the status of MS context sharing with the peer node and no matter whether keep-alive initiation functionality is enabled or disabled on this node.

The MSID field in the header of *Keep-alive RSP* message SHALL be set to Zero.

1 The NE SHALL always include Last Reset Time TLV in the Keep-alive RSP message with the value that was set  
2 right after the last boot up.

3 When the NE receives Keep-alive Req message, it MAY check the received LRT value (the receiver of Keep-alive  
4 Req message is not mandated to keep track of the peer that sends the message). If the LRT value received in *Keep-*  
5 *alive Req* message does not match the stored non-zero value for the peer node, the receiver of the message SHALL  
6 consider the peer node has passed restart during the time interval from the last keep-alive interrogation. Note that it  
7 may take the appropriate action, which is implementation specific.

8 When NE receives *Keep-alive Req* from the peer it does not maintain any shared contexts for the MS with, it MAY  
9 cache the peer's IP address/ Identity and its corresponding LRT value.

10 NE that does not support Keep-alive functionality, SHALL follow error handling procedure as specified in the  
11 section 3.4 to signal the sender its inability to support Keep-alive.

## 12 4.18 Application Server Discovery

13 The following describes the procedures on how the MS discovers the address(es) of Application Server(s) in order to  
14 initiate sessions for specific applications. The described procedure is valid for following applications:

- 15 • Location Server for the Location Based Service as specified in [LBS-SPEC].

16 During IP address acquisition at network entry, the MS/ Application Client MAY send DHCP Request with a DHCP  
17 Option [IETF RFC 2132] to acquire the Application Server address(es) or a list of FQDN of the Application  
18 Server(s) (AS) for different kind of applications.

19 If MS has not requested the Application Server address(es) using DHCP Request during IP address acquisition at  
20 network entry, the MS SHALL send DHCP Inform with a DHCP Option [IETF RFC 2132] to acquire the  
21 Application server address(es) or a list of FQDN of the Application Server(s) after IP address acquisition.

22 If MS has requested the Application Server address(es) using DHCP Request and obtained the same using DHCP  
23 Ack message, then the MS SHALL NOT send DHCP INFORM with a DHCP Option to obtain Application Server  
24 address(es).

### 25 4.18.1 DHCP Proxy in the ASN

26 The NAS MAY receive the address(es) and/or a list of fully qualified domain names (FQDN) of Application  
27 Server(s) from the HAAA server during the successful User Access Authentication. The information SHALL be  
28 stored in the DHCP Proxy within the ASN.

29 MS MAY indicate to the ASN that it wants Application Server address or FQDN list of Application Server in the  
30 DHCP Request message during IP address acquisition. Accordingly, the DHCP Proxy MAY optionally include the  
31 address(es) of the Application Server(s) in the DHCP Ack.

32 If the DHCP Inform message from the MS for the address(es) or a FQDN list of Application Server has been  
33 received, the DHCP Proxy SHALL acknowledge the address(es) or a FQDN list of the Application Server(s) by  
34 sending the DHCP Ack message to the MS as defined in RFC 2131 for IPv4 or RFC 3315 for IPv6.

### 35 4.18.2 DHCP Relay in the ASN

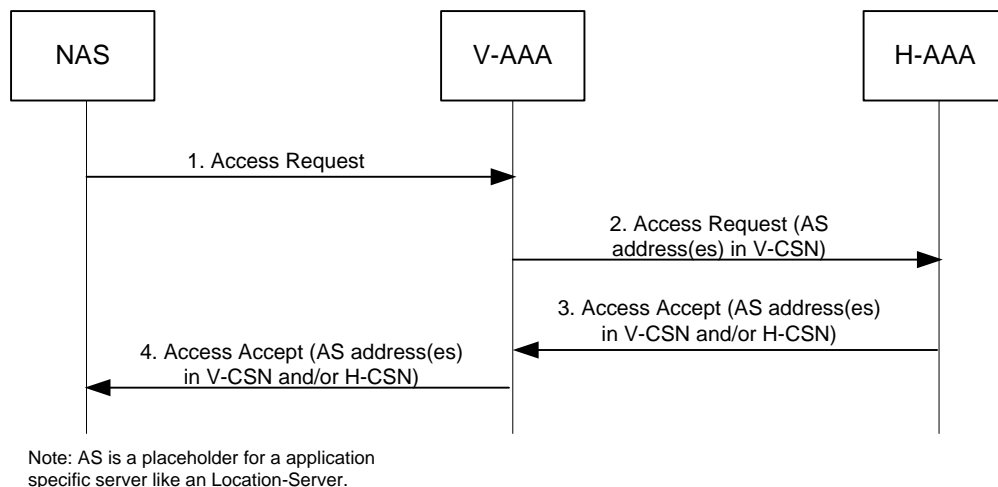
36 The MS MAY indicate to the ASN that it wants Application Server address or FQDN list of Application Server in  
37 the DHCP Request message during IP address acquisition. Accordingly, the DHCP Server MAY include the  
38 address(es) or FQDN list of the Application Server(s) in the DHCP Ack.

39 If the DHCP INFORM message from the MS for the address(es) or a FQDN list of Application Server has been  
40 received, the DHCP Relay SHALL relay the message to the DHCP Server. The DHCP Server MAY learn the  
41 address or FQDN of Application Server from AAA server.

42 Upon receiving the acknowledge the address(es) or a FQDN list of the Application Server(s) from the DHCP Server  
43 as defined in RFC 2131 for IPv4 or RFC 3315 for IPv6, the DHCP Relay SHALL relay the DHCP ACK message to  
44 the MS.

### 4.18.3 Server Discovery for Roaming Users

In a roaming case, the Application Server (i.e., LS) address can be assigned by either the Home NSP or the Visited NSP. For Server(s) in the Visited CSN, the Visited AAA proxy can append the Server address(es) or FQDNs in the AAA exchange messages between the ASN and the Home AAA server. It's the Home AAA that will finally decide, based on the roaming agreement with the visited operator and/or the end-user's subscription profile, which network is responsible for assigning the Servers and assign the appropriate Server address(es) or a FQDNs in the Home AAA reply to the ASN. The Home AAA should assign the Server and other entities (i.e., DHCP server, DNS server) to be collocated within the same network (Home NSP or Visited NSP) to the MS.



**Figure 4-188 – AS Discovery (Roaming Scenario)**

#### STEP 1

When the NAS gets the access authentication request from the MS, the NAS sends the RADIUS Access-Request message to the Visited AAA proxy in the Visited CSN.

#### STEP 2

The Visited AAA proxy forwards the RADIUS Access-Request message to the Home AAA server. The Visited AAA MAY append the Server (i.e., LS) address(es) or FQDNs belonging to the Visited CSN in this message prior to forwarding to the Home AAA server (if local network policy allows).

#### STEP 3

The Home AAA server assigns the Server address(es) or FQDNs in the RADIUS Access-Accept message and sends the RADIUS Access-Accept to the Visited AAA. The Server address assigned by the Home AAA server can either be the one available in the home network or the one provided by the Visited AAA proxy or both. The HAAA decides this depending on the roaming agreement and/or the end-user subscription profile. The Home AAA MUST assign at least one Application Server per functionality in the RADIUS Access-Accept if application service (e.g. location service) is authorized for that subscriber.

#### STEP 4

The Visited AAA proxy forwards the RADIUS Access-Accept message including the AS address(es) (e.g. of an LBS Server) to the NAS.

## 5. Message and Parameter Definitions

### 5.1 Constants and Counters

This section defines constants and counters used in the specification.

#### 5.1.1 CMAC\_Key\_Count Counter

#### 5.1.2 CMAC Packet Number Counter

#### 5.1.3 CMAC\_PN\_\* Counter

#### 5.1.4 Entry Counter

#### 5.1.5 HO\_Req Retransmission Limit

#### 5.1.6 R6 HO\_Req Retry Counter

### 5.2 Message Definitions and Construction Rules

The following provides guidance for constructing and documenting a message definition.

1. A child TLV SHALL NOT appear in a message definition without its parent TLV also appearing in the message definition.
2. If a child TLV that is optional in the parent's TLV definition appears as Mandatory in a message definition, then its parent TLV SHALL also appear as Mandatory in the message definition.
3. If a parent TLV appears as Mandatory in a message definition, all of its Mandatory child TLVs (as shown in the parent TLV definition) SHALL also appear as Mandatory in the message definition.
4. If a parent TLV appears as Optional in a message definition, all of its Mandatory child TLVs (as shown in the parent TLV definition) SHALL appear as Conditional Mandatory in the message definition. Each of these child TLVs SHALL include the note: This TLV SHALL be included if the *insert name of parent TLV* is included in the transmitted message.

**Table 5-1 – Function and Message Types Index**

Function Type	Msg Type	OP ID	Message	Message Layout
1 (QoS)	1	001	<i>RR_Req</i>	Table 4-32, Table 4-59, Table 4-60, Table 4-61, Table 4-62, Table 4-63
	2	010	<i>RR_Rsp</i>	Table 4-33, Table 4-64, Table 4-65,
	3	011	<i>RR_Ack</i>	Table 4-66
2 (HO Control)	1	001	<i>HO_Req</i>	Table 4-82, Table 4-104, Table 4-111, Table 4-113
	2	010	<i>HO_Rsp</i>	Table 4-85



Function Type	Msg Type	OP ID	Message	Message Layout
	3	011 for the 3-way Handshake and 010 in case of 2-way transaction	<i>HO_Ack</i>	Table 4-86
	4	001	<i>HO_Cnf</i>	Table 4-90, Table 4-91
	5	001	<i>HO_Complete</i>	Table 4-99
	6	001	<i>HO_Directive</i>	
	7	010	<i>HO_Directive_Rsp</i>	
3 (Data Path Control)	1	001	<i>Path_Dereg_Req</i>	Table 4-35, Table 4-51, Table 4-75
	2	010	<i>Path_Dereg_Rsp</i>	Table 4-76
	3	011	<i>Path_Dereg_Ack</i>	This message does not contain any TLVs, so there is no message layout.
	4	001	<i>Path_Modification_Req</i>	Table 4-72
	5	010	<i>Path_Modification_Rsp</i>	Table 4-73
	6	011	<i>Path_Modification_Ack</i>	Table 4-74
	7	001	<i>Path_Prereg_Req</i>	Table 4-87
	8	010	<i>Path_Prereg_Rsp</i>	Table 4-88
	9	011	<i>Path_Prereg_Ack</i>	Table 4-89
	10	001	<i>Path_Reg_Req</i>	Table 4-94
	11	010	<i>Path_Reg_Rsp</i>	Table 4-95
	12	011	<i>Path_Reg_Ack</i>	Table 4-96, Table 4-172, Table 4-177
	13	100	<i>IM_Exit_State_Ind</i>	Table 4-175
	14	011	<i>IM_Exit_State_Ind_Ack</i>	Table 4-176
4 (Context Transfer)	1	001	<i>Context_Req</i>	Table 4-83, Table 4-156
	2	010 (for the report sent in response to <i>Context_Req</i> message) and 001 (Report sent without <i>Context_Req</i> message and waiting for <i>Context_Ack</i> message)	<i>Context_Rpt</i>	Table 4-20, Table 4-31, Table 4-84, Table 4-157, Table 4-116
	3	010	<i>Context_Ack</i>	Table 4-21, Table 4-117
	4	001	<i>CMAC_Key_Count_Up date</i>	Table 4-97

Function Type	Msg Type	OP ID	Message	Message Layout
	5	010	<i>CMAC_Key_Count_Up date_Ack</i>	Table 4-98
	6	-	<i>VOID</i>	
	7	-	<i>VOID</i>	
	8	001	<i>Prepaid Request</i>	This message does not contain any TLVs, so there is no message layout.
	9	010	<i>Prepaid Notify</i>	This message does not contain any TLVs, so there is no message layout.
5 (R3 Mobility)	1	001	<i>Anchor_DPF_HO_Req</i>	Table 4-113, Table 4-133
	2	100	<i>Anchor_DPF_HO_Trig ger</i>	Table 4-114
	3	010	<i>Anchor_DPF_HO_Rsp</i>	Table 4-115
	4	001	<i>Anchor_DPF_Relocate _Req</i>	Table 4-118
	5	010	<i>Anchor_DPF_Relocate _Rsp</i>	Table 4-121
	6	001	<i>FA_Register_Req</i>	Table 4-119
	7	010	<i>FA_Register_Rsp</i>	Table 4-120
	8	001	<i>FA_Revoke_Req</i>	Table 4-124
	9	010	<i>FA_Revoke_Rsp</i>	Table 4-125
	10	001	<i>Anchor_DPF_Release_ Req</i>	This message does not contain any TLVs, so there is no message layout.
	11	001	<i>Relocation_Ready_Req</i>	This message does not contain any TLVs, so there is no message layout.
	12	010	<i>Relocation_Ready_Rsp</i>	This message does not contain any TLVs, so there is no message layout.
6 (Paging)	1	100	<i>Paging_Announce</i>	Table 4-164, Table 4-165
	2	001	<i>Delete_MS_Entry_Req</i>	This message does not contain any TLVs, so there is no message layout.
	3	100	<i>PC_Relocation_Ind</i>	Table 4-158
	4	011	<i>PC_Relocation_Ack</i>	Table 4-159
	5	010	<i>Delete_MS_Entry_Rsp</i>	This message does not contain any TLVs, so there is no message layout.

Function Type	Msg Type	OP ID	Message	Message Layout
	6	100	<i>Anchor_PC_Ind</i>	Table 4-183
	7	011	<i>Anchor_PC_Ack</i>	Table 4-184
7 (RRM)	1	001	R6 <i>PHY_Parameters_Req</i> (used in Release 1.0 only)	
	2	010	R6 <i>PHY_Parameters_Rpt</i> (used in Release 1.0 only)	
	3	001	<i>Spare_Capacity_Req</i>	Table 4-144
	4	010 (for the report send for <i>Spare_Capacity_Req</i> message) and 100 (for periodic or event-driven reporting without request)	<i>Spare_Capacity_Rpt</i>	Table 4-145
	5	100	R6 <i>Neighbor_BS_Resource_Status_Update</i> (used in Release 1.0 only)	
	6	001	<i>Radio_Config_Update_Req</i>	Table 4-146
	7	010 (for the report send for <i>Radio_Config_Update_Req</i> message) and 100 (Report sent as an Indication and waiting for <i>Radio_Config_Update_Ack</i> message)	<i>Radio_Config_Update_Rpt</i>	Table 4-147
	8	011 for the 3-way Handshake and 010 in case of 2-way transaction	<i>Radio_Config_Update_Ack</i>	Table 4-148
8 (Authentication Relay)	1	100	<i>AR_EAP_Start</i>	Table 4-8
	2	100	<i>AR_EAP_Transfer</i>	Table 4-9
	3	001	<i>Bulk Interim Update</i>	Table 4-34
	4	010	<i>Bulk Interim Update_Ack</i>	This message does not contain any TLVs, so there is no message layout.

Function Type	Msg Type	OP ID	Message	Message Layout
9 (MS State)	1	001	<i>MS_PreAttachment_Req</i>	Table 4-42
	2	010	<i>MS_PreAttachment_Rsp</i>	Table 4-43
	3	011	<i>MS_PreAttachment_Ack</i>	Table 4-44
	4	001	<i>MS_Attachment_Req</i>	Table 4-46
	5	010	<i>MS_Attachment_Rsp</i>	Table 4-47
	6	011	<i>MS_Attachment_Ack</i>	This message does not contain any TLVs, so there is no message layout.
	7	001	<i>Key_Change_Directive</i>	Table 4-10
	8	001	<i>Key_Change_Cnf</i>	Table 4-11
	9	010	<i>Key_Change_Ack</i>	Table 4-12
	10	001	<i>Relocation_Complete_Req</i>	This message does not contain any TLVs, so there is no message layout.
	11	010	<i>Relocation_Complete_Rsp</i>	This message does not contain any TLVs, so there is no message layout.
	12	011	<i>Relocation_Complete_Ack</i>	This message does not contain any TLVs, so there is no message layout.
	13	001	<i>Relocation_Notify</i>	Table 4-13,
	14	001	<i>Relocation_Req</i>	Table 4-18
	15	010	<i>Relocation_Rsp</i>	Table 4-19
	16	001	<i>NetExit_MS_State_Change_Req</i>	Table 4-52
	17	010	<i>NetExit_MS_State_Change_Rsp</i>	Table 4-53
	18	010	<i>Relocation_Notify_Rsp</i>	Table 4-14
10 IM Operations	1	001	<i>IM_Entry_State_Change_Req</i>	Table 4-35, Table 4-182, Table 4-185
	2	010	<i>IM_Entry_State_Change_Rsp</i>	Table 4-186
	3	011	<i>IM_Entry_State_Change_Ack</i>	Table 4-187
	4	001	<i>IM_Exit_State_Change_Req</i>	Table 4-170, Table 4-173
	5	010	<i>IM_Exit_State_Change_Rsp</i>	Table 4-32, Table 4-171, Table 4-174

Function Type	Msg Type	OP ID	Message	Message Layout
	6	001	<i>Initiate_Paging_Req</i>	Table 4-162
	7	010	<i>Initiate_Paging_Rsp</i>	Table 4-163
	8	001	<i>LU_Req</i>	Table 4-153
	9	010	<i>LU_Rsp</i>	Table 4-154
	10	011	<i>LU_Cnf</i>	Table 4-155
11 Accounting	1	001	<i>Hotlining_Req</i>	Table 4-40
	2	010	<i>Hotlining_Rsp</i>	Table 4-41
14 R4R6R8_Capability	1	001	<i>Capability_Req</i>	Table 4-190
	2	010	<i>Capability_Rsp</i>	Table 4-191
	3	011	<i>Capability_Ack</i>	Table 4-192
15 General (not MS specific)	1	001	<i>Keep-alive_Req</i>	Table 4-193
	2	010	<i>Keep-alive_Rsp</i>	Table 4-194

## 5.3 TLV Definitions

### 5.3.1 TLV Format

The format of TLV appears below:

00	01						07								15											23							31
T	C	Type														Length																	
Value (actual number of octets in the Value Field is specified in the value of the Length Field)																																	

The type field defines the type of data element. It is 15 bits long. The type field is preceded by the TC bit at bit position 0 (the most significant bit of the first octet) in transmission bit order. The TC bit has the following meaning (for further information, cf. section 3.5.1):

- If the TC bit is set to 0, TLV comprehension is required;
- If the TC bit is set to 1, TLV comprehension is not required.

Note: For usage of the TC bit in messages sent to a legacy node, see Annex *Hooks and Principles for Evolution* [2].

The Length field defines the length of the value portion in octets (thus a TLV with no value portion would have a length of zero). The Type equal to 0x7FFF is reserved for vendor-specific extensions. All other undefined type codes are reserved for future assignment. The value field itself could contain other TLVs, and such TLVs are termed nested TLVs.

In the following TLV definitions that include child TLVs, a child TLV SHALL be shown either as optional (O), or mandatory (M).

- If a child TLV is shown as O in the TLV definition, then if the child TLV is included in a message, it SHALL be shown as either O or M in the message. The choice depends upon the requirements of the message.

- If a child TLV is shown as M in the TLV definition, then if the child TLV is included in a message, it SHALL be shown either as CM (conditional mandatory) or M in the message. CM is used when the parent TLV is shown as O in the message. It indicates that the child TLV is included in the message if its parent TLV is included in the message. M is used in all other cases.

### 5.3.2 TLV Encoding

All enumeration values start from 0 unless specified otherwise.

In the definition of TLVs, the following terms are used:

Reserved bit                      The sender SHALL set a reserved bit to 0. The receiver SHALL ignore a reserved bit.

Reserved value                      The sender SHALL NOT use a reserved value; the receiver SHALL consider a reserved value as erroneous.

#### 5.3.2.1 Accept/Reject Indicator

<b>Type</b>	1
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = accept</li> <li>• 0x01 = reject</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates Accept/Reject of the corresponding request.
<b>Parent TLV(s)</b>	None

#### 5.3.2.2 Accounting Extension

<b>Type</b>	2
<b>Length in octets</b>	Variable
<b>Value</b>	String
<b>Description</b>	This parameter indicates information relevant for accounting. The operation and the application content provider determine the format and value of the Accounting Extension.
<b>Parent TLV</b>	SF Info

### 5.3.2.3 Action Code

<b>Type</b>	3
<b>Length in octets</b>	2
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x0000 = Deregister MS. MS SHALL immediately terminate service with the BS and should attempt network entry at another BS;</li> <li>• 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;</li> <li>• 0x0002 = Suspend user traffic (transport connections). MS SHALL listen to the current BS but only transmit on the Basic and Primary Management Connections;</li> <li>• 0x0003 = Resume traffic. MS SHALL return to normal operation and may transmit on any of its active connections.</li> <li>• 0x0005 = MS SHALL be put into idle mode.</li> <li>• 0xffffe = Initial Authentication Failure. MS SHALL be sent the RNG-RSP with Ranging Result Code = Abort by the BS.</li> <li>• 0xffff = MS SHALL be sent the RES-CMD by the BS. The MS will reload all configuration information and do initial network entry.</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	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.
<b>Message Primitives That Use This TLV</b>	Path Control messages ( <i>Path_Dereg_Req</i> ), MS State Change messages.

### 5.3.2.4 Action Time

<b>Type</b>	4
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	For HO, this value indicates the radio frame in which the Target BS allocates a dedicated transmission opportunity for RNG-REQ message to be transmitted by the MS using Fast Ranging IE. This value is defined in absolute number of radio frames.
<b>Parent TLV(s)</b>	BS Info

### 5.3.2.5 AK

<b>Type</b>	5
<b>Length in octets</b>	20
<b>Value</b>	160-bit AK Value.
<b>Description</b>	AK is derived from the PMK at the NAS.
<b>Parent TLV(s)</b>	AK Context

1 **5.3.2.6 AK Context**

<b>Type</b>	6	
<b>Length in octets</b>	Variable but not less than 10	
<b>Value</b>	Compound	
<b>Description</b>	Contains AK Context from Authenticator.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	AK	M
	AK ID	M
	AK Lifetime	M
	AK SN	M
	CMAC_KEY_COUNT	M
<b>Parent TLV(s)</b>	BS Info	

2 **5.3.2.7 AK ID**

<b>Type</b>	7
<b>Length in octets</b>	8
<b>Value</b>	64-bit AK ID Value.
<b>Description</b>	Identifies the AK that is used for protecting the message.
<b>Parent TLV(s)</b>	AK Context

3 **5.3.2.8 AK Lifetime**

<b>Type</b>	8
<b>Length in octets</b>	4
<b>Value</b>	32-bit AK Lifetime value in seconds.
<b>Description</b>	The time period during which the AK will be valid.
<b>Parent TLV(s)</b>	AK Context

4 **5.3.2.9 AK SN**

<b>Type</b>	9
<b>Length in octets</b>	1
<b>Value</b>	The field is coded as follows: 4-bit Reserved   4-bit AK SN.
<b>Description</b>	The Sequence number of root keys (PMK) for the AK.
<b>Parent TLV(s)</b>	AK Context



1 **5.3.2.10 Anchor ASN GW ID**

<b>Type</b>	10
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets)
<b>Value</b>	The Identifier might be in format of either a 4-octet IPv4 Address, a 6-octet IEEE 802.16 BS ID or a 16-octet IPv6 Address. The length defines also the format of the Identifier.
<b>Description</b>	Unique identifier for the Anchor GW / Anchor Data Path Function.
<b>Parent TLV(s)</b>	MS Info

2 **5.3.2.11 Anchor MM Context**

Type	11	
Length in octets	Variable	
Value	Compound	
Description	Information related with FA/MAG relocation, which means all context maintained by some entities binding with FA/MAG 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
	PMIP6 Info	O
Parent TLV	MS Info	

3 **5.3.2.12 Anchor PC ID**

<b>Type</b>	12
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets)
<b>Value</b>	The Identifier might be in format of either a 4-octet IPv4 Address, a 6-octet IEEE 802.16 BS ID or a 16-octet IPv6 Address. The length defines also the format of the Identifier.
<b>Description</b>	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.
<b>Parent TLV(s)</b>	Paging Information, IDLE Mode Info.

1 **5.3.2.13 Anchor PC Relocation Destination**

2 Exists if relocation is requested.

<b>Type</b>	13
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets)
<b>Value</b>	Destination might be in the format of either a 4-octet IPv4 address, a 6-octet 802.16 BS ID or a 16-octet IPv6 address. The length defines the format of the identifier.
<b>Description</b>	Network identifier for a new (target) Anchor Paging Controller network entity, which administers paging activity for the MS while in Idle Mode and retains MS service and operational information.
<b>Parent TLV(s)</b>	Paging Information

3 **5.3.2.14 Anchor PC Relocation Request Response**

4 Exists if relocation is requested.

<b>Type</b>	14
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Accept</li> <li>• 0x01 = Refuse</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates Accept/Reject of the corresponding request.
<b>Parent TLV(s)</b>	Paging Information

5 **5.3.2.15 Associated PHSI**

<b>Type</b>	15
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	The Associated PHSI value. It SHALL be equal to the PHSI value of the corresponding PHS Rule.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

1 **5.3.2.16 FA Revoke Reason**

<b>Type</b>	16
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = DHCP Release</li> <li>• 0x01 = DHCP expiry</li> <li>• 0x02 = FA initiated release</li> <li>• 0x03 = HA initiated release</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates the FA Revoke Reason.
<b>Message Primitives That Use This TLV</b>	FA Revoke Req

2 **5.3.2.17 Authentication Complete**

Type	17		
Length in octets	2		
Value	Compound		
Description			
Elements (Sub-TLVs)	TLV Name		M/O
	Authentication Result		M
	PKM2 Message Code		M
Message Primitives That Use This TLV	Key_Change_Directive		

3 **5.3.2.18 Authentication Result**

<b>Type</b>	18
<b>Length in octets</b>	1
<b>Value</b>	<ul style="list-style-type: none"> <li>• Enumerator. The values are: 0x00 = Success</li> <li>• 0x01 = Failure</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	This parameter indicates to BS the results of EAP authentication process.
<b>Parent TLV(s)</b>	Authentication Complete, MS Info

#### 1 5.3.2.19 Authenticator ID

<b>Type</b>	19
<b>Length in octets</b>	Variable (could be of three fixed sizes: 4, 6 and 16 octets)
<b>Value</b>	The Identifier might be in format of either a 4-octet IPv4 Address, a 6-octet IEEE 802.16 BS ID or a 16-octet IPv6 Address. The length defines also the format of the Identifier.
<b>Description</b>	Unique identifier of MS's Anchor Authenticator.
<b>Parent TLV(s)</b>	MS Info

#### 2 5.3.2.20 RRQ

<b>Type</b>	20
<b>Length in octets</b>	Variable
<b>Value</b>	Same as defined in [48] including IP/UDP headers.
<b>Description</b>	MIP Register Request message defined in [48].
<b>Parent TLV(s)</b>	FA_Register_Req

3 Note [a]: Used only during HO/ Idle Mode entry/exit operations.

#### 4 5.3.2.21 Authorization Policy Support

<b>Type</b>	21
<b>Length in octets</b>	1
<b>Value</b>	<p>8-bit Bitmask coded as follows:</p> <ul style="list-style-type: none"> <li>• Bit #0 = RSA-based authorization at the initial network entry</li> <li>• Bit #1 = EAP-based authorization at the initial network entry</li> <li>• Bit #2 = Authenticated EAP-based authorization at the initial network entry</li> <li>• Bit #4 = RSA-based authorization at reentry</li> <li>• Bit #5 = EAP-based authorization at reentry</li> <li>• Bit #6 = Authenticated EAP-based authorization at reentry</li> </ul> <p>All other bits are Reserved.</p>
<b>Description</b>	This parameter is used to indicate authentication mode. In MS Security History TLV, it indicates the capability negotiated between ASN and MS. Refer to 11.8.4.2 Authorization policy support in 802.16e.
<b>Parent TLV</b>	MS Security History, Security Negotiation Parameters

1 **5.3.2.22 Available Radio Resource DL**

<b>Type</b>	22
<b>Length in octets</b>	1
<b>Value</b>	<p>8-bit unsigned integer:</p> <ul style="list-style-type: none"> <li>• 0x00 = 0%</li> <li>• 0x01 = 1%,</li> <li>• ...,</li> <li>• 0x64 = 100%</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Available Radio Resource indicator DL SHALL indicate the average ratios of non assigned DL resources to the total usable DL radio resources. The average in percentage SHALL take place over a time interval specified by Averaging Time TLV of RRM <i>Spare_Capacity_Req</i> if provided; if omitted, the BS SHALL apply a default value.
<b>Parent TLV(s)</b>	RRM BS Info

2 **5.3.2.23 Available Radio Resource UL**

<b>Type</b>	23
<b>Length in octets</b>	1
<b>Value</b>	<p>8-bit unsigned integer:</p> <ul style="list-style-type: none"> <li>• 0x00 = 0%</li> <li>• 0x01 = 1%,</li> <li>• ...,</li> <li>• 0x64 = 100%</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Available Radio Resource indicator UL SHALL indicate the average ratios of non assigned DL resources to the total usable DL radio resources. The average in percentage SHALL take place over a time interval specified by Averaging Time TLV of RRM <i>Spare_Capacity_Req</i> if provided; if omitted, the BS SHALL apply a default value.
<b>Parent TLV(s)</b>	RRM BS Info

1 **5.3.2.24 BE Data Delivery Service**

<b>Type</b>	24	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	This compound TLV contains the QoS parameters relevant for BE Data Delivery Service. If included in QoS Parameters, it implies BE Scheduling Service for UL connections.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Maximum Sustained Traffic Rate	O
	Traffic Priority	O (if omitted means Traffic Priority = 0)
	Request/Transmission Policy	O [a]
<b>Parent TLV</b>	QoS Parameters	

2 Note: [a] – Used during Service flow creation, HO/ Idle Mode entry/ exit operations.

3 **5.3.2.25 BS ID**

<b>Type</b>	25
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets)
<b>Value</b>	The Identifier might be in format of either a 4-octet IPv4 Address, a 6-octet IEEE 802.16 BS ID or a 16-octet IPv6 Address. The length defines also the format of the Identifier.
<b>Description</b>	Unique BS Identifier, referring to a single sector with a single frequency assignment.
<b>Parent TLV(s)</b>	BS Info, RRM BS Info

1 **5.3.2.26 BS Info**

<b>Type</b>	26	
<b>Length in octets</b>	Variable	
<b>Value</b>		
<b>Description</b>	Description of BS.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	BS ID	M
	Serving/Target Indicator	O <sup>21</sup>
	Round Trip Delay	O
	Relative Delay	O
	DL PHY Quality Info	O
	UL PHY Quality Info	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
	Time Stamp	O
	BS HO RSP Code	O
	AK Context	O (Note 1)
	BS Location	O
	Reattachment Zone	O
<b>Message Primitives That Use This TLV</b>	Every Message	

2 Note: HO ID is defined in the IEEE 802.16e spec.

3 1)AK Context SHALL be included as sub-TLV of BS Info in the following messages:

- 4 a. Key\_Change\_Directive Message in order to transfer the new security context (AK Context) to BS and
- 5 trigger the PKMv2 3-WHS process between the BS and the MS.
- 6 b. Context\_Rpt from authenticator ASN to Target ASN.
- 7 c. May be included in HO-Req message.

<sup>21</sup> Serving/Target Indicator is conditionally mandatory. See tables in section 4.

1 **5.3.2.27 BS-originated EAP-Start Flag**

<b>Type</b>	27
<b>Length in octets</b>	0
<b>Value</b>	N/A
<b>Description</b>	Flag indicating that <i>AR_EAP_Start</i> message is originated by a BS (without receiving PKMv2 EAP-Start from an MS). A BS may use <i>AR_EAP_Start</i> with this flag to instigate reauthentication process when MS security context in BS is going to expire.
<b>Parent TLV</b>	MS Info

2 **5.3.2.28 Care-of Address (CoA)**

<b>Type</b>	28
<b>Length in octets</b>	4
<b>Value</b>	Care-of Address (CoA) of the MS.
<b>Description</b>	
<b>Parent TLV(s)</b>	MIP4 Info

3 **5.3.2.29 CID/MCID**

<b>Type</b>	29
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	CID/MCID definition as per 802.16.
<b>Parent TLV(s)</b>	SF Info

4 **5.3.2.30 Classification Rule Index**

<b>Type</b>	30
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	This TLV defines the index assigned to this classification rule: <ul style="list-style-type: none"> <li>• The index is unique per service flow.</li> </ul>
<b>Parent TLV(s)</b>	Packet Classification Rule / Media Flow Description



1 **5.3.2.31 Classification Rule Action**

<b>Type</b>	31
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Add Classification Rule,</li> <li>• 0x01 = Replace Classification Rule,</li> <li>• 0x02 = Delete Classification Rule.</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Add, replace or delete the classification Rule for the classification of a specific service flow.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

2 **5.3.2.32 Classification Rule Priority**

<b>Type</b>	32
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	The value of the field specifies the priority for the Classification Rule, which is used for determining the order of the Classification Rule. A higher value indicates higher priority. Classification Rules may have priorities in the range 0–255 with the default value being 0.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

3 **5.3.2.33 Void**

4 **5.3.2.34 CMAC\_KEY\_COUNT**

<b>Type</b>	34
<b>Length in octets</b>	2
<b>Value</b>	Unsigned 16-bit integer.
<b>Description</b>	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.
<b>Parent TLV(s)</b>	AK Context
	MS Info

1 **5.3.2.35 Combined Resources Required**

<b>Type</b>	35
<b>Length in octets</b>	2
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x0000 = Not combined;</li> <li>• 0x0001 =Combined;</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	<p>When this TLV's value is "Combined," then if any of the pre-provisioned SFs for the indicated CS type cannot be successfully established, all of the SFs for the CS type must be removed. When this TLV's value is "Not combined," then each pre-provisioned SF for the indicated CS type can be established independently,</p> <p>If the CS Type TLV indicates "All CS Types," then this TLV applies to all pre-provisioned SFs for the MS.</p> <p>Absence of this TLV is interpreted as if the TLV's value is set to 0x0000.</p>
<b>Parent TLV</b>	Combined Resource Indicator

2 **5.3.2.36 Context Purpose Indicator**

<b>Type</b>	36
<b>Length in octets</b>	4
<b>Value</b>	<p>32-bit Bitmask.</p> <ul style="list-style-type: none"> <li>• Bit #0 = MS AK Context.</li> <li>• Bit #1 = MS Network Context</li> <li>• Bit #2 = MS MAC Context</li> <li>• Bit #3 = MS Authorization Context</li> <li>• Bit #4 = Anchor MM Context</li> <li>• Bit #5 = Accounting context</li> <li>• Bit #6 = MS Security History</li> <li>• Bit #7 = SA Context</li> <li>• Bit #8 = MN-FA key context</li> <li>• Bit #9 = FA-HA key context</li> <li>• Bit #10 = DHCP-Relay-Info</li> <li>• Bit #11 = Security Context Delivery</li> <li>• Bit #12 = MIP6 handover successful</li> <li>• Bit #13 = Online Accounting context</li> <li>• Bit #14 = Offline Accounting context</li> </ul> <p>All other bits are Reserved.</p>

<b>Description</b>	<p>Indicates the type of context to be delivered:</p> <ul style="list-style-type: none"> <li>• Setting Bit #0 requests delivering AK Context associated with a particular MS.</li> <li>• Setting Bit #1 requests or reports 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.</li> <li>• Setting Bit#2 requests delivery of MAC Context associated with a particular MS that is available in BS. This includes REG Context, SBC Context and PKMv2 context.</li> <li>• Setting Bit#3 requests delivery of service authorization and policy context (e.g., authorization code) associated with a particular MS.</li> <li>• Setting Bit#4 requests delivery of Anchor MM Context associated with a particular MS.</li> <li>• Setting Bit#5 requests delivery of Accounting provisioning info</li> <li>• Setting Bit#6 requests delivery of MS Security History</li> <li>• Setting Bit#7 requests SA Context. This is included based on the bits set in the Idle Mode Retain Information TLV from the MS and if cached in the BS apriori.</li> <li>• Setting Bit#7 requests delivery of MIP4 Security Info TLV with MN-FA key context.</li> <li>• Setting Bit#9 requests delivery of MIP4 Security Info TLV with FA-HA key context.</li> <li>• Setting Bit#10 requests delivery of DHCP relay information.</li> <li>• Setting Bit#11 requests delivery of the security context.</li> <li>• Setting bit#12 indicates that the MIP6 handover is successfully completed and R4 data path between previous anchor DPF and new anchor DPF can be released.</li> <li>• Setting Bit#13 requests delivery of Online Accounting context/ quota(s).</li> <li>• Setting Bit#14 requests delivery of Offline Accounting context.</li> </ul>
<b>Message Primitives That Use This TLV</b>	Context Delivery messages.

#### 1 5.3.2.37 Correlation ID

<b>Type</b>	37
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	<p>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.</p>
<b>Parent TLV(s)</b>	SF Info

### 1 5.3.2.38 Cryptographic Suite

<b>Type</b>	38
<b>Length in octets</b>	4
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00000 = No data encryption, no data authentication &amp; 3-DES, 128</li> <li>• 0x010001 = CBC-Mode 56-bit DES, no data authentication &amp; 3-DES, 128</li> <li>• 0x000002 = No data encryption, no data authentication &amp; RSA, 1024</li> <li>• 0x010002 = CBC-Mode 56-bit DES, no data authentication &amp; RSA, 1024</li> <li>• 0x020103 = CCM-Mode 128-bit AES, CCM-Mode, 128-bit, ECB mode AES with 128-bit key</li> <li>• 0x020104 = CCM-Mode 128bits AES, CCM-Mode, AES Key Wrap with 128-bit key</li> <li>• 0x030003 = CBC-Mode 128-bit AES, no data authentication, ECB mode AES with 128-bit key</li> <li>• 0x800003 = MBS CTR Mode 128 bits AES, no data authentication, AES ECB mode with 128-bit key</li> <li>• 0x800004 = MBS CTR mode 128 bits AES, no data authentication, AES Key Wrap with 128-bit key</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates cryptographic suites allowed.
<b>Parent TLV(s)</b>	SA Descriptor

### 2 5.3.2.39 CS Type

<b>Type</b>	39
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = All CS Types</li> <li>• 0x01 = Packet, IPv4</li> <li>• 0x02 = Packet, IPv6</li> <li>• 0x03 = Packet, 802.3</li> <li>• 0x04 = void</li> <li>• 0x05 = void</li> <li>• 0x06 = void</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates type of convergence layer between MS and BS.
<b>Parent TLV(s)</b>	SF Info, Combined Resource Indicator

#### 5.3.2.40 Data Integrity

<b>Type</b>	40
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = No recommendation</li> <li>• 0x01 = Data integrity requested</li> <li>• 0x02 = Data delay jitter sensitive</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Specifies, if data integrity is recommended. The value “data integrity requested” advises the base station that mechanisms like ARQ/HARQ are requested. The value “data delay jitter sensitive” advises the base station, that ARQ/HARQ may have negative effects.
<b>Parent TLV</b>	QoS Parameters

#### 5.3.2.41 PMIP-Authenticated-Network-Identity

<b>Type</b>	41
<b>Length in octets</b>	Variable up to 256 octets
<b>Value</b>	ASCII String
<b>Description</b>	PMIP Network Access Identifier character string
<b>Parent TLV(s)</b>	MS Security History, MS Authorization Context, MIP4 Security Info
<b>Message Primitives That Use This TLV</b>	Context Request

#### 5.3.2.42 Data Path Encapsulation Type

<b>Type</b>	42
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x01 = GRE</li> <li>• 0x02 = VOID</li> <li>• 0x03 = VOID</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Data Path Type.
<b>Parent TLV</b>	Data Path Info

#### 5.3.2.43 Void

#### 5.3.2.44 Data Path ID

<b>Type</b>	44
<b>Length in octets</b>	4
<b>Value</b>	Data Path Identifier (e.g., GRE Key).

<b>Description</b>	Identifier for a data path.
<b>Parent TLV</b>	Data Path Info

1 **5.3.2.45 Data Path Info**

<b>Type</b>	45	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Data Path Description.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Data Path ID	M
	Data Path Encapsulation Type	O
	Data Path Type	O
	Tunnel Endpoint	O
	ARQ Window Info	O
<b>Parent TLV</b>	SF Info (for per SF Data Path)	

2 **5.3.2.46 Void**

3 **5.3.2.47 Data Path Type**

<b>Type</b>	47
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>0x01 = Type1</li> <li>0x02 = Type2</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Distinguishes between Type 1 and Type 2 datapaths.
<b>Parent TLV</b>	Data Path Info

4 **5.3.2.48 DCD/UCD Configuration Change Count**

<b>Type</b>	48
<b>Length in octets</b>	1
<b>Value</b>	<p>8-bit integer:</p> <ul style="list-style-type: none"> <li>Bits #0...3 = The 4 LSBs of the BS's current DCD configuration change count;</li> <li>Bits #4...7 = The 4 LSBs of the BS's current UCD configuration change count.</li> </ul>
<b>Description</b>	This includes the 4 LSBs of the BS's current DCD and UCD configuration change count figures
<b>Parent TLV(s)</b>	RRM BS Info

5 **5.3.2.49 DCD Setting**

<b>Type</b>	49
-------------	----

<b>Length in octets</b>	Variable
<b>Value</b>	Compound, as specified in [802.16e-2005], section 11.1.7.
<b>Description</b>	<p>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.</p> <p>The DCD setting 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.</p> <p>See [802.16e-2005], section 11.1.7.</p>
<b>Parent TLV(s)</b>	RRM BS Info

#### 1 5.3.2.50 ODFMA Parameters Sets

<b>Type</b>	50
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask
<b>Description</b>	<p>Identifies the profile of the capabilities of the MS negotiated during SBC handshake</p> <ul style="list-style-type: none"> <li>• Bit#0 = Support OFDMA PHY parameter set A</li> <li>• Bit#1 = Support OFDMA PHY parameter set B</li> <li>• Bit#2-#4 = HARQ parameters set <ul style="list-style-type: none"> <li>– 0b000 = HARQ set 1</li> <li>– 0b001 = HARQ set 2</li> <li>– 0b010 = HARQ set 3</li> <li>– 0b011 = HARQ set 4</li> <li>– 0b100 = HARQ set 5</li> <li>– 0b101-0b111 = Reserved</li> </ul> </li> <li>• Bit#5 = Support OFDMA MAC parameters set A</li> <li>• Bit#6 = Support OFDMA MAC parameters set B</li> <li>• Bit#7 = Reserved</li> </ul> <p>Note: Bit#0 and #1 SHALL not be set to 1 together. Bit#5 and #6 SHALL not be set to 1 together.</p>
<b>Parent TLV</b>	SBC Context

#### 2 5.3.2.51 DHCP Key

<b>Type</b>	51
<b>Length in octets</b>	20
<b>Value</b>	160-bit unsigned integer.
<b>Description</b>	<p>Key used to calculate and authenticate messages between the DHCP relay in the ASN and DHCP server in the CSN, as per [65]. This TLV SHALL be included in the <i>Context_Rpt</i> message (as part of DHCP Relay Info TLV) if Context Purpose Indicator TLV was set to DHCP-Relay-Info.</p>

<b>Parent TLV(s)</b>	DHCP Relay Info
----------------------	-----------------

1 **5.3.2.52 DHCP Key ID**

<b>Type</b>	52
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Key ID associated with the key used to compute authentication suboption as per [65]. This TLV SHALL be included in the <i>Context_Rpt</i> message (as part of DHCP Relay Info TLV) if DHCP Key TLV is included.
<b>Parent TLV(s)</b>	DHCP Relay Info

2 **5.3.2.53 DHCP Key Lifetime**

<b>Type</b>	53
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	The remaining lifetime in seconds of the DHCP key. This TLV SHALL be included in the <i>Context_Rpt</i> message (as part of DHCP Relay Info TLV) if DHCP Key TLV is included.
<b>Parent TLV(s)</b>	DHCP Relay Info

3 **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	
	DHCP Proxy Type	O	
	DNS IP Address	O	
Parent TLV(s)	Anchor MM Context		

4 **5.3.2.55 DHCP Relay Address**

<b>Type</b>	55
<b>Length in octets</b>	Variable (either 4 or 16 bytes)
<b>Value</b>	IPv4 or IPv6 address.
<b>Description</b>	DHCP relay's IPv4 or IPv6 address facing the DHCP server. This TLV SHALL be included in the <i>Context_Req</i> message (as part of DHCP Relay Info TLV) if Context Purpose Indicator TLV is set to DHCP-Relay-Info.
<b>Parent TLV(s)</b>	DHCP Relay Info



1 **5.3.2.56 DHCP Relay Info**

<b>Type</b>	56	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Information about the DHCP Relay. This TLV SHALL be included in the <i>Context_Req</i> and <i>Context_Rpt</i> messages if Context Purpose Indicator TLV is set to DHCP-Relay-Info.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	DHCP Server Address	O
	DHCP Relay Address	O
	DHCP Key	O
	DHCP Key ID	O
	DHCP Key Lifetime	O
<b>Parent TLV(s)</b>	<i>MS Info.</i>	

2 **5.3.2.57 DHCP Server Address**

<b>Type</b>	57	
<b>Length in octets</b>	Variable (either 4 or 16 )	
<b>Value</b>	IPv4 or IPv6 address.	
<b>Description</b>	IPv4 or IPv6 address of the DHCP server. This TLV SHALL be included in the <i>Context_Rpt</i> message (as part of DHCP Relay Info TLV) if Context Purpose Indicator TLV was set to DHCP-Relay-Info. This TLV may be included multiple times as part of the DHCP Server List TLV.	
<b>Parent TLV(s)</b>	DHCP Relay Info and DHCP Server List	

3 **5.3.2.58 DHCP Server List**

<b>Type</b>	58	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	List of DHCP servers.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	DHCP Server Address	O
<b>Parent TLV(s)</b>	Anchor MM Context	

1 **5.3.2.59 Direction**

<b>Type</b>	59
<b>Length in octets</b>	2
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>0x0000 = For Uplink</li> <li>0x0001 = For Downlink</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Describes the unidirectional Service Flow direction (i.e., UL or DL).
<b>Parent TLV</b>	SF Info

2 **5.3.2.60 DL PHY Quality Info**

<b>Type</b>	60
<b>Length in octets</b>	4
<b>Value</b>	32-bit integer encoding 8-bit DL RSSI Mean, 8-bit DL RSSI Std, 8-bit DL CINR Mean, 8-bit DL CINR Std.
<b>Description</b>	
<b>Parent TLV</b>	BS Info, RRM BS-MS PHY Quality Info

3 **5.3.2.61 DL PHY Service Level**

<b>Type</b>	61
<b>Length in octets</b>	4
<b>Value</b>	32-bit integer representing DL PSL.
<b>Description</b>	
<b>Parent TLV</b>	RRM BS-MS PHY Quality Info

4 **5.3.2.62 EAP Payload**

<b>Type</b>	62
<b>Length in octets</b>	Variable
<b>Value</b>	EAP Payload (for EAP over R6 Authentication Relay).
<b>Description</b>	EAP Messages.
<b>Message Primitives That Use This TLV</b>	EAP Relay messages

1 **5.3.2.63 Void**

2 **5.3.2.64 ERT-VR Data Delivery Service**

<b>Type</b>	64	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	This compound TLV contains the QoS parameters relevant for ERT-VR Data Delivery Service. If included in QoS Parameters, it implies ertPS Scheduling Service for UL connections.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O Flag</b>
	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
<b>Parent TLV</b>	QoS Parameters	

3 Note [a]: Used during Service flow creation, HO/ Idle Mode entry/exit operations.

4 **5.3.2.65 PPAC**

<b>Type</b>	65	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	The PrepaidAccountingCapability (PPAC) TLV is sent by a prepaid capable ASN entity and is used to describe the prepaid capabilities of the ASN.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O Flag</b>
	AvailableInClient	M
<b>Message Primitives that use this TLV</b>	Relocation_Complete_Rsp, Anchor_DPF_HO_Trigger, Anchor_DPF_HO_Req	

#### 1 5.3.2.66 FA-HA Key

<b>Type</b>	66
<b>Length in octets</b>	20
<b>Value</b>	160-bit unsigned integer.
<b>Description</b>	Using FA-HA key to calculate and authenticate FA-HA-AE, integrity can be protected between HA and FA.
<b>Parent TLV(s)</b>	MIP4 Security Info

#### 2 5.3.2.67 FA-HA Key Lifetime

<b>Type</b>	67
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Time of FA-HA key remaining valid.
<b>Message Primitives That Use This TLV</b>	MIP4 Security Info

#### 3 5.3.2.68 FA-HA Key SPI

<b>Type</b>	68
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Key ID of FA-HA key. It should be equal to the SPI (Key ID) of HA-RK.
<b>Message Primitives That Use This TLV</b>	MIP4 Security Info

#### 4 5.3.2.69 Failure Indication

<b>Type</b>	69
<b>Length in octets</b>	1 byte
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Unspecified Error</li> </ul> <p>Error Codes: 0x01-0x0F Message Header Failure Codes</p> <ul style="list-style-type: none"> <li>• 0x01 = Protocol Version not understood (note 1)</li> <li>• 0x02 = Unrecognized Function Type</li> <li>• 0x03 = Invalid Message Type</li> <li>• 0x04 = Unknown MSID</li> <li>• 0x05 = Transaction Failure</li> <li>• 0x06 = Source Identifier unknown or inconsistent with the IP source address</li> <li>• 0x07 = Destination unknown</li> <li>• 0x08 = Invalid Message Header</li> <li>• 0x09 = Invalid OP ID</li> </ul>

	<ul style="list-style-type: none"> <li>• 0x0A = Destination Identifier missing or erroneous</li> <li>• 0x0B = Source Identifier TLV missing or erroneous</li> <li>• 0x0C = Message type unknown or inopportune</li> <li>• 0x0D = Unresolved error</li> <li>• 0x0E-0x0F = Unspecific Message Header Failure; the sender SHALL NOT use the value. The receiver, when receiving this value, SHALL understand this value as “Unspecific Message Header Failure”.</li> </ul> <p>Error Codes: 0x10-0x1F General Message Body Failure Codes</p> <ul style="list-style-type: none"> <li>• 0x10 = Invalid message format</li> <li>• 0x11 = Mandatory TLV missing</li> <li>• 0x12 = TLV Value Invalid</li> <li>• 0x13 = Unsupported Options</li> <li>• 0x14 = TLV Unknown</li> <li>• 0x15 = TLV Unexpected</li> <li>• 0x16 = TLV parsing error</li> <li>• 0x17-0x1F = Unspecific General Message Body Failure; the sender SHALL NOT use the value. The receiver, when receiving this value, SHALL understand this value as “Unspecific General Message Body Failure”.</li> </ul> <p>Error Codes: 0x20-0x2F Message Generic Failure Codes</p> <ul style="list-style-type: none"> <li>• 0x20 = Timer expired without response</li> <li>• 0x21 = BSID out of service</li> <li>• 0x22 = Unknown BSID</li> <li>• 0x23 = BSID Unreachable</li> <li>• 0x24-0x2F = Unspecific Message Generic Failure; the sender SHALL NOT use the value. The receiver, when receiving this value, SHALL understand this value as “Unspecific Message Generic Failure”.</li> </ul> <p>Error Codes: 0x30-0x7F Message-specific Failure Codes</p> <ul style="list-style-type: none"> <li>• 0x30 = Requested Context Unavailable</li> <li>• 0x31 = Authorization Failure</li> <li>• 0x32 = Registration Failure</li> <li>• 0x33 = No Resources</li> <li>• 0x34 = Failure by rejection of MS</li> <li>• 0x35 = Authenticator relocated</li> <li>• 0x36 = Does not support periodic reporting of RRM messages</li> <li>• 0x37 = Location Update Failure</li> <li>• 0x38 = Idle Mode Authorization Failure</li> <li>• 0x39 = Target BS doesn’t support this HO Type</li> <li>• 0x3A = Insufficient Target BS airlink resource</li> <li>• 0x3B = Target BS CPU overload</li> <li>• 0x3C = Out of MS Reattachment Zone</li> <li>• 0x3D-0x7F = Unspecific Message-specific Failure; the sender SHALL NOT use the value. The receiver, when receiving this value, SHALL understand this value as “Unspecific Message-specific Failure”</li> </ul> <p>(To be updated with sub section team specific error handling)</p>
--	---

	<p>Error codes: 0x80-0xFE: Unspecific Failure; the sender SHALL NOT use the value. The receiver, when receiving this value, SHALL understand this value as “Unspecific Failure”.</p> <p>Error Code 0xFF is reserved to indicate use of an error extension field. The sender SHALL NOT use the value. The receiver, when receiving this value, SHALL understand this value as “Unspecific Failure”.</p>
<b>Description</b>	<p>Indicates the reason for failure of a previous message</p> <p>The sender SHALL include the Failure Indication TLV in the <i>first free position after the header</i> (see section 3.5.2) of a normal response or ACK message if the failure of the previous message of the same transaction has to be indicated. The sender SHALL include the Failure Indication TLV in the <i>first free position after the header</i> (see section 3.5.2) of each Error Response or Error Reflection message (see section 3.5.2).</p>
<b>Parent TLV</b>	None
<b>Message Primitives That Use This TLV</b>	Any message on R6/R4/R8 that is used for failure reporting.

- 1 Note 1: This value might be used by legacy entities to indicate that a message with Protocol Version different from 1  
2 has been received. The value should be blocked for any other use in protocol version 1.

### 3 5.3.2.70 Target FA IP Address

<b>Type</b>	70
<b>Length in octets</b>	4
<b>Value</b>	IP address of the entity which containing an FA function.
<b>Description</b>	
<b>Parent TLV(s)</b>	MIP4 Info

### 4 5.3.2.71 FA Relocation Indication

<b>Type</b>	71
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Success</li> <li>• 0x01 = Failure</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	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”.
<b>Parent TLV(s)</b>	MS Info

### 1 5.3.2.72 Full DCD Setting

<b>Type</b>	72
<b>Length in octets</b>	Variable
<b>Value</b>	Compound, as specified in [802.16e-2005], section 11.1.7.
<b>Description</b>	This is an IEEE802.16e-2005 defined TLV. The DCD_setting 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.
<b>Parent TLV(s)</b>	RRM BS Info

### 2 5.3.2.73 Full UCD Setting

<b>Type</b>	73
<b>Length in octets</b>	Variable
<b>Value</b>	Compound, as specified in [802.16e-2005], section 11.1.7.
<b>Description</b>	This is an IEEE802.16e-2005 defined TLV. The UCD_setting 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.
<b>Parent TLV(s)</b>	RRM BS Info

### 3 5.3.2.74 Global Service Class Name

<b>Type</b>	74
<b>Length in octets</b>	6
<b>Value</b>	Global Service Class Name as defined in IEEE802.16e.
<b>Description</b>	Provides an authorized QoS parameters set in a length optimized format.
<b>Parent TLV(s)</b>	QoS Parameters, R3 QoS Descriptor

### 4 5.3.2.75 HA IP Address

<b>Type</b>	75
<b>Length in octets</b>	Variable (either 4 or 16)
<b>Value</b>	IP address of HA. The Identifier might be in format of either a 4-octet IPv4 Address or a 16-octet IPv6 Address. The length defines also the format of the Identifier.
<b>Description</b>	
<b>Parent TLV(s)</b>	MIP4 Info, MIP4 Security Info

1 **5.3.2.76 HO Confirm Type**

<b>Type</b>	76
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are Enumerator:</p> <ul style="list-style-type: none"> <li>• 0x00 = Confirm</li> <li>• 0x01 = Unconfirm</li> <li>• 0x02 = Cancel</li> <li>• 0x03 = Reject</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	<p>Indicates whether one of the candidate BSs is selected as the HO target or not.</p> <p>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.</p>
<b>Message Primitives That use this TLV</b>	HO_Cnf

2 **5.3.2.77 Home Address (HoA)**

<b>Type</b>	77
<b>Length in octets</b>	4
<b>Value</b>	Home Address (HoA) of the MS. In case of PMIP6 it is the IPv4 MN-HoA
<b>Description</b>	
<b>Parent TLV(s)</b>	MIP4 Info, PMIP6 Info

3 **5.3.2.78 HO Process Optimization**

<b>Type</b>	78
<b>Length in octets</b>	1
<b>Value</b>	8-bit integer representing HO Process Optimization code.
<b>Description</b>	
<b>Parent TLV</b>	BS Info, RRM BS Info



### 1 5.3.2.79 HO Type

<b>Type</b>	79
<b>Length in octets</b>	4
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00000000 = Hard Handoff (HHO)</li> <li>• 0x00000001 = Fast Base Station Switching (FBSS)</li> <li>• 0x00000002 = Macro Diversity Handoff (MDHO)</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Allows communication of various handover types.
<b>Message Primitives That Use This TLV</b>	HO Control messages

### 2 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
Parent TLV(s)	Anchor MM Context	

### 3 5.3.2.81 IDLE Mode Retain Info

<b>Type</b>	81
<b>Length in octets</b>	1
<b>Value</b>	
<b>Description</b>	Indicates which re-entry management messages SHALL be retained and managed. Encoded as in 802.16e.
<b>Parent TLV(s)</b>	Paging Information

### 4 5.3.2.82 IP Destination Address and Mask

<b>Type</b>	82
<b>Length in octets</b>	8 (IPv4) or 32 (IPv6).
<b>Value</b>	An IP Destination Address/Mask pairs: (dst1, dmask).
<b>Description</b>	An IP destination addresses and its corresponding address mask. An IP packet with IP destination address “ip-dst” matches this parameter if Dst = (ip-dst AND Dmask). If this parameter is omitted, then comparison of the IP packet destination address for this entry is irrelevant.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

1 **5.3.2.83 IP Remained Time**

<b>Type</b>	83
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Remaining lease time for the assigned IP address, indicated in second.
<b>Message Primitives That Use This TLV</b>	DHCP Proxy Info

2 **5.3.2.84 IP Source Address and Mask**

<b>Type</b>	84
<b>Length in octets</b>	8 (IPv4) or 32 (IPv6)
<b>Value</b>	An IP Source Address/Mask pairs: (Src1, Smask).
<b>Description</b>	An IP source address and its corresponding address mask. An IP packet with IP source address “ip-src” matches this parameter if Src = (ip-src AND Smask). If this parameter is omitted, then comparison of the IP packet source address for this entry is irrelevant.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

3 **5.3.2.85 IP TOS/DSCP Range and Mask**

<b>Type</b>	85
<b>Length in octets</b>	3
<b>Value</b>	The value field is structured as follows: <ul style="list-style-type: none"> <li>• Octet 1: Lower Limit</li> <li>• Octet 2: Higher Limit</li> <li>• Octet 3: Mask</li> </ul>
<b>Description</b>	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.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

1 **5.3.2.86 Key Change Indicator**

<b>Type</b>	86
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>0x00 = Success</li> <li>0x01 = Failure</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	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.
<b>Parent TLV(s)</b>	MS Info

2 **5.3.2.87 L-BSID**

<b>Type</b>	87
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets).
<b>Value</b>	The Identifier might be in format of either a 4-octet IPv4 Address, a 6-octet IEEE 802.16 BS ID or a 16-octet IPv6 Address. The length defines also the format of the Identifier.
<b>Description</b>	Unique BS Identifier, referring to a single sector with a single frequency assignment.
<b>Message Primitives That Use This TLV</b>	R4_Paging_Announce

3 **5.3.2.88 Location Update Status**

<b>Type</b>	88
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. Supported values in this release:</p> <ul style="list-style-type: none"> <li>0x00 = Accept</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates successful location update result.
<b>Parent TLV(s)</b>	Paging Information

#### 5.3.2.89 AvailableInClient

<b>Type</b>	89
<b>Length in octets</b>	4
<b>Value</b>	4 Octet String interpreted as a bit map with the following values: <ul style="list-style-type: none"> <li>• 0x00000000 = Reserved</li> <li>• 0x00000001 = Volume metering supported</li> <li>• 0x00000002 = Duration metering supported</li> <li>• 0x00000004 = Resource metering supported</li> <li>• 0x00000008 = Pools supported</li> <li>• 0x00000010 = Rating groups supported</li> <li>• 0x00000020 = Multi-Services supported</li> <li>• 0x00000040 = Tariff Switch supported</li> </ul> All other values are Reserved.
<b>Description</b>	AvailableInClient TLV indicates the metering capabilities of the ASN and SHALL be bitmap encoded.
<b>Parent TLV(s)</b>	PPAC

#### 5.3.2.90 LU Result Indicator

<b>Type</b>	90
<b>Length in octets</b>	1
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"> <li>• 0x00 = Success</li> <li>• 0x01 = Failure</li> </ul> All other values are Reserved.
<b>Description</b>	Boolean that indicates the result of the LU operation.
<b>Message Primitives That Use This TLV</b>	PC_Relocation_Ind

#### 5.3.2.91 Maximum Latency

<b>Type</b>	91
<b>Length in octets</b>	4
<b>Value</b>	32-bit integer specifies the maximum latency (in milliseconds).
<b>Description</b>	Time period between the reception of a packet by the BS or MS on its network interface and the delivering of 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.
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>• UGS Data Delivery Service</li> <li>• ERT-VR Data Delivery Service</li> <li>• RT-VR Data Delivery Service</li> </ul>

### 1 5.3.2.92 Maximum Sustained Traffic Rate

<b>Type</b>	92
<b>Length in octets</b>	4
<b>Value</b>	32-bit integer representing rate (in bits per second).
<b>Description</b>	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.
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>• ERT-VR Data Delivery Service</li> <li>• RT-VR Data Delivery Service</li> <li>• NRT-VR Data Delivery Service</li> <li>• BE Data Delivery Service</li> <li>• UGS Data Delivery Service</li> <li>• R3 Qos Descriptor</li> </ul>

### 2 5.3.2.93 Maximum Traffic Burst

<b>Type</b>	93
<b>Length in octets</b>	4
<b>Value</b>	32-bit integer representing burst size (in bytes).
<b>Description</b>	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.
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>• ERT-VR Data Delivery Service</li> <li>• RT-VR Data Delivery Service</li> <li>• NRT-VR Data Delivery Service</li> <li>• R3 QoS Descriptor</li> </ul>

### 3 5.3.2.94 Media Flow Type

<b>Type</b>	94
<b>Length in octets</b>	1

<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x01 = Voice over IP</li> <li>• 0x02 = Robust Browser</li> <li>• 0x03 = Secure Browser/ VPN</li> <li>• 0x04 = Streaming video on demand</li> <li>• 0x05 = Streaming live TV</li> <li>• 0x06 = Music and Photo Download</li> <li>• 0x07 = Multi-player gaming</li> <li>• 0x08 = Location-based services</li> <li>• 0x09 = Text and Audio Books with Graphics</li> <li>• 0x0A = Video Conversation</li> <li>• 0x0B = Message</li> <li>• 0x0C = Control</li> <li>• 0x0D = Data</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
<b>Parent TLV</b>	QoS Parameters

1 **5.3.2.95 Minimum Reserved Traffic Rate**

<b>Type</b>	95
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer representing rate (in bits per second).
<b>Description</b>	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.
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>• UGS Data Delivery Service</li> <li>• ERT-VR Data Delivery Service</li> <li>• RT-VR Data Delivery Service</li> <li>• NRT-VR Data Delivery Service</li> <li>• R3 Qos Descriptor</li> </ul>

2 **5.3.2.96 MIP4 Info**

Type	96		
Length in octets	Variable		
Value	Compound		
Description	MIP4 Information about the MS.		
Elements (Sub-	TLV Name		M/O

<b>TLVs)</b>	Target FA IP Address	O
	Target Care-of Address	O
	HA IP Address	O
	Home Address (HoA)	O
	Care-of Address (CoA)	O
	Registration Lifetime	O
	Downlink R3 GRE Key	O
	Uplink R3 GRE Key	O
<b>Parent TLV(s)</b>	Anchor MM Context, PMIP4 Context	

1 **5.3.2.97 RRP**

<b>Type</b>	97
<b>Length in octets</b>	variable
<b>Value</b>	Same as defined in [48] including IP/UDP headers.
<b>Description</b>	MIP Register Response message defined in [48].
<b>Message Primitives That Use This TLV</b>	FA_Register_Rsp

2 **5.3.2.98 MN-FA Key**

<b>Type</b>	98
<b>Length in octets</b>	20
<b>Value</b>	160-bit unsigned integer.
<b>Description</b>	Using MN-FA key to calculate and authenticate MN-FA-AE, integrity can be protected between MN and FA.
<b>Parent TLV(s)</b>	MIP4 Security Info

3 **5.3.2.99 MN-FA SPI**

<b>Type</b>	99
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Key ID of MN-FA key.
<b>Parent TLV(s)</b>	MIP4 Security Info

4 **5.3.2.100MS Authorization Context**

<b>Type</b>	100
<b>Length in octets</b>	Variable
<b>Value</b>	Compound

Description		
Elements (Sub-TLVs)	TLV Name	M/O
	MS NAI	M
	PMIP-Authenticated-Network-Identity	O
	R3 WiMAX Capability	M
	R3 CUI	O
	R3 Class	O
	R3 Framed IP Address	O
	R3 Framed-IPv6-Prefix	O
	R3 Framed-Interface-Id	O
	R3 Visited-Framed-IP-Address	O
	R3 Visited-Framed-IPv6-Prefix	O
	R3 Visited-Framed-Interface-Id	O
	R3 WiMAX Session ID	M
	R3 Packet Flow Descriptor	M
	R3 QoS Descriptor	O
	R3 Acct Interim Interval	O
	Authorized Network Services	O <sup>1</sup>
	Visited Authorized Network Services	O
	Certified-MS-Feature-List-For-GW	O <sup>2</sup>
	Certified-MS-Feature-List-For-BS	O <sup>3</sup>
Parent TLV	MS Info	

Note 1: Authorized Network Services SHALL be sent from the old Authenticator to the new Authenticator during Authenticator Relocation procedure; in the R4 Relocation Request or R4 Relocation Complete Response message in case of Authenticator Relocation push; in the R4 Relocation Notify Response or R4 Relocation Complete Response in case of Authenticator Relocation Pull. Refer to Stage 3.

Note 2: This TLV SHALL be present if Certified-MS-Feature-List-for-GW is received as part of RADIUS/DIAMETER message.

Note 3: This TLV SHALL be present if Certified-MS-Feature-List-for-BS is received as part of RADIUS/DIAMETER message.

### 5.3.2.101 Target Care-of Address

Type	101
Length in octets	4
Value	
Description	
Parent TLV(s)	MIP4 Info



### 5.3.2.102 MSID

<b>Type</b>	102
<b>Length in octets</b>	6
<b>Value</b>	48-bit MS MAC address.
<b>Description</b>	Unique MS identifier (MS MAC address) (Note 1).
<b>Parent TLV(s)</b>	MS Info, Accounting Bulk Session/Flow

Note 1: An MSID with all bits set to zero has a specific meaning, see section 3.1.

### 5.3.2.103 MS Info<sup>22</sup>

<b>Type</b>	103	
<b>Length in octets</b>	Length of MS Info is set as ‘Variable’.	
<b>Value</b>	Compound	
<b>Description</b>	Information about the MS.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	MSID	O
	SF Info	O (Note 1)
	PPAQ	O
	Anchor ASN GW ID	O (Note 2)
	Authenticator ID	O (Note 3)
	SA Descriptor	O
	Service Authorization Code	O
	REG Context	O
	SBC Context	O
	Anchor MM Context	O (Note 4)
	MS Security History	O (Note 5)
	MS Authorization Context	O (Note 6)
	Combined Resource Indicator	O
	Authentication Result	O (Note 7)
	DHCP Relay Info	O
	FA Relocation Indication	O
	BS-originated EAP-Start Flag	O
	CMAC_KEY_COUNT	O
	VLAN Tag Processing Rule	O (Note 8)
	Key Change Indicator	O (Note 9)

<sup>22</sup> 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.

	State	O (Note 10)
	MS MAC Version	O
	NSP ID	O
	Data Integrity Capability	O
	Mobility Access Classifier	O
	Reattachment Zone	O
	LBS Loc Info	O
	LBS Transaction ID	O
	LBS Result Code	O
<b>Message Primitives That Use This TLV</b>	Every Message	

## Notes

- One or more SF Info TLVs MAY be included in order to describe Service Flows in Data Path Control, Reservation, and HO Control Messages. Data Path Control SF Info is included for Per-SF data path tunneling granularity. SF Info TLV is Mandatory in HO\_Req message in Mobility. See section 4.7.2.1.
- Anchor ASN GW ID points to the network entity that hosts Anchor DP Function.
  - It MAY be included as sub-TLV of MS Info in *HO\_Req* message in order to inform the Target ASN (or Target BS) about the location of the network entity that hosts Anchor DP Function.
  - Anchor ASN GW ID MAY be included as sub-TLV of MS Info in Data Path Control messages in order to inform the peer about the location of the network entity that hosts Anchor DP Function.
  - It MAY be included as sub-TLV of MS Info in Context Delivery messages.
- Authenticator GW ID points to the network entity that hosts Authenticator Function.
  - It MAY be included as sub-TLV of MS Info in *HO\_Req* message in order to inform the Target ASN (or Target BS) about the location of the network entity that hosts Authenticator Function. It doesn't have to be included if AK Context is included. If neither Authenticator GW ID nor AK Context is included, it means that the sender of the *HO\_Req* hosts the Authenticator Function for the MS.
  - Authenticator GW ID MAY be included as sub-TLV of MS Info in Data Path Control messages in order to inform the peer about the location of the network entity that hosts Authenticator Function.
  - It MAY be included as sub-TLV of MS Info in Context Delivery messages.
- MIP4 Info TLV SHALL be included as sub-TLV of Anchor MM Context during the Authenticator Relocation Procedure defined in section 4.4.1.5.5 in the Relocation\_Notify\_Rsp and Relocation\_Req messages sent from the old Authenticator to the new Authenticator.
- MS Security History is mandatory when MS Info is included in Relocation\_Notify message.
- MS Authorization Context is mandatory when MS Info is included in Relocation\_Notify\_Rsp and Relocation\_Req messages.
- Authentication Result is mandatory when MS Info is included in Relocation\_Complete message.
- If used for prepaid accounting, present with PPAQ to continue prepaid accounting session.
- Key Change Indicator is mandatory when MS Info is included in Key\_Change\_Cnf message or MS\_Attachment\_Req message.
- VLANTagProcessingRule exists only for ETH-CS

1 **5.3.2.104MS Mobility Mode**

<b>Type</b>	104
<b>Length in octets</b>	2 byte
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x0000 = PMIP4</li> <li>• 0x0001 = CMIP4</li> <li>• 0x0002 = CMIP6</li> <li>• 0x0003 = PMIP6</li> <li>• 0x0004 = MIP based ETH</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates which R3 mobility the MS is using.
<b>Parent TLV(s)</b>	Anchor MM Context

2 **5.3.2.105MS NAI**

<b>Type</b>	105
<b>Length in octets</b>	Variable up to 256 octets
<b>Value</b>	ASCII String.
<b>Description</b>	MS Network Access Identifier character string.
<b>Parent TLV(s)</b>	MS Security History, MIP4 Security Info, MS Authorization Context

3 **5.3.2.106MS MAC Version**

<b>Type</b>	106
<b>Length in octets</b>	1
<b>Value</b>	1 Byte value
<b>Description</b>	Indicates MS MAC Version per IEEE 802.16 standard. The MAC Version Value is, indicated in TLV-148 during Network entry. When the MAC value is larger than 6, the MS is indicating support for ND&S.
<b>Parent TLV(s)</b>	MS Info

### 5.3.2.107 Void

### 5.3.2.108 MS Security History

<b>Type</b>	108	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>	Security parameters presenting the history of MS authentication.	
<b>Elements (Bus-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	PMK SN	O
	MS NAI	O
	PMIP-Authenticated-Network-Identity	O
	Authorization Policy Support	O [Note 1]
	VAAA Realm	O [Note 2]
	VAAA IP Address	O [Note 2]
<b>Parent TLV(s)</b>	MS Info	

Note 1: Authorization policy support TLV in MS Security History indicates the authentication modes as previously negotiated with MS. in Authenticator Relocation procedure.

Note 2: If MS is re-authenticating via the visited CSN, either VAAA Realm or VAAA IP Address TLV SHALL be present.

### 5.3.2.109 Network Exit Indicator

<b>Type</b>	109
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>0x00 = MS Power Down indication (used if Network Exit Indicator is requested in RNG REQ).</li> <li>0x01 = Radio link with MS is lost.</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Present in operations related to MS Network Exit and indicates MS Network Exit reason.
<b>Parent TLV(s)</b>	Path Control messages ( <i>Path_Dereg_Req</i> ), MS State Change messages.

1 **5.3.2.110 Newer TEK Parameters**

<b>Type</b>	110	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>	Set of the Newer TEK Parameters.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	TEK	M
	TEK SN	M
	TEK Lifetime	M
	PN Counter	O
	RxPN Counter	O
<b>Parent TLVs</b>	SA Descriptor	

2 **5.3.2.111 NRT-VR Data Delivery Service**

<b>Type</b>	111	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	This compound TLV contains the QoS parameters relevant for NRT-VR Data Delivery Service. If included in QoS Parameters, it implies nrtPS Scheduling Service for UL connections.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	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
<b>Parent TLV</b>	QoS Parameters	

3 Note [a]: Used during Service flow creation, HO/ Idle Mode entry/exit operations.

1 **5.3.2.112 Older TEK Parameters**

<b>Type</b>	112	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>	Set of the Older TEK Parameters.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	TEK	M
	TEK SN	M
	TEK Lifetime	M
	PN Counter	O
	RxPN Counter	O
<b>Parent TLVs</b>	SA Descriptor	

2 **5.3.2.113 Old Anchor PC ID**

<b>Type</b>	113
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets)
<b>Value</b>	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 a 4-octet IPv4 Address, a 6-octet IEEE 802.16 BS ID or a 16-octet IPv6 Address. The length defines also the format of the Identifier.
<b>Description</b>	
<b>Parent TLV(s)</b>	Paging Information

3 **5.3.2.114 Packet Classification Rule / Media Flow Description (one or more)**

<b>Type</b>	114	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Contains sub-elements representing Classification 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.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Classification Rule Index	M
	Classification Rule Action Note: The Classification Rule Action is mandatory for service flow modification; and it does not apply to the service flow creation or deletion.	O
	Classification 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
	Classification Result	O
	MAC Source Address and Mask	O <sup>1</sup>
	MAC Destination Address and Mask	O <sup>1</sup>
	ETYPE/SAP	O <sup>1</sup>
	User Priority Range	O <sup>1</sup>
	SVLAN Range	O <sup>1,2</sup>
	CVLAN Range	O <sup>1,3</sup>
<b>Parent TLV</b>	SF Info	

1 Note 1: These TLVs are valid only when the CS TYPE in SF INFO is ETH-CS.

2 Note 2: The SVLAN Range is only used in downlink classification in ASN.

3 Note 3: The CVLAN Range is used as VLAN Range in uplink.

#### 4 5.3.2.115 Paging Announce Timer

<b>Type</b>	115
<b>Length in octets</b>	2 octet
<b>Value</b>	16-bit unsigned integer (in seconds).
<b>Description</b>	<p>The duration which the MS should be paged.</p> <p>Paging Announce timer = 0xFFFF means that a PagingAgent SHALL apply its internal timer value and/or algorithm. The PagingAgent will continue paging the MS until it receives a Paging::Stop message for the MS, or the internal timer value expires, or an implementation-specific algorithm decides to stop the paging – whichever comes first.</p> <p>PagingAnnounce timer = 0 stands for a single page.</p> <p>PagingAnnounce timer &gt; 0 implies that the Paging Agent will page the MS until this timer value (in seconds) expires.</p> <p>If PagingAnnounce timer is omitted, then a value of 0 is assumed.</p>
<b>Parent TLV(s)</b>	Paging Information

1 **5.3.2.116Paging Cause**

<b>Type</b>	116
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x01 = Location update.</li> <li>• 0x02 = Network Re-Entry, Incoming Data for Idle MS.</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	
<b>Parent TLV(s)</b>	Paging Information

2 **5.3.2.117Relay PC ID**

<b>Type</b>	117
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets).
<b>Value</b>	<p>Unique identifier for the Paging Controller network entity, which partakes in forwarding of Idle mode and Paging related network messages between the MS and Anchor PC and vice versa. May take part in PC relocation during MS Location Update process. Relay PC can be the identifier of serving ASN when the MS Anchor PC is not in serving ASN.</p> <p>The Identifier has same format as Anchor PC ID.</p>
<b>Description</b>	
<b>Parent TLV(s)</b>	Paging Information

3 **5.3.2.118Paging Cycle**

<b>Type</b>	118
<b>Length in octets</b>	2
<b>Value</b>	
<b>Description</b>	Cycle in which the paging message is transmitted within the paging group (aligned with 802.16e).
<b>Parent TLV(s)</b>	Paging Information



1 **5.3.2.119Paging Information**

<b>Type</b>	119	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>	Set of Paging related IEs.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Paging Cycle	O
	Paging Offset	O
	Paging Interval Length	O
	Relocation Success Indicator	O
	Paging Group ID	O
	Relay PC ID	O
	Anchor PC ID	O
	IDLE Mode Retain Info	O
	Paging Start/Stop	O
	Anchor PC Relocation Destination	O
	Anchor PC Relocation Request Response	O
	Location Update Status	O
	Paging Cause	O
	Idle Mode Timeout	O
	Old Anchor PC ID	O
	Paging Announce Timer	O
<b>Message Primitives That Use This TLV</b>	Paging Function messages; Data Path Control messages; Context Delivery messages.	

2 **5.3.2.120Paging Offset**

<b>Type</b>	120
<b>Length in octets</b>	2
<b>Value</b>	
<b>Description</b>	Determines the frame within the cycle in which the paging message is transmitted. SHALL be smaller than the PAGING CYCLE value.
<b>Parent TLV(s)</b>	Paging Information

1 **5.3.2.121 Paging Start/Stop**

<b>Type</b>	121
<b>Length in octets</b>	1
<b>Value</b>	
<b>Description</b>	Indicates to the BSs whether to start/stop paging on the airlink.
<b>Parent TLV(s)</b>	Paging Information

2 **5.3.2.122 PC Relocation Indication**

<b>Type</b>	122
<b>Length in octets</b>	1
<b>Value</b>	
<b>Description</b>	Request from the Current Anchor PC to the New Anchor PC to perform PC relocation.
<b>Message Primitives That Use This TLV</b>	R4 <i>LU_Rsp</i>

3 **5.3.2.123 Paging Group ID**

<b>Type</b>	123
<b>Length in octets</b>	2
<b>Value</b>	Byte string
<b>Description</b>	16-bit ID representing Paging Group.
<b>Parent TLV(s)</b>	Paging Information

4 **5.3.2.124 PHSF**

<b>Type</b>	124
<b>Length in octets</b>	Variable
<b>Value</b>	Byte string
<b>Description</b>	String of bytes containing the header information to be suppressed.
<b>Parent TLV</b>	PHS Rule

5 **5.3.2.125 PHSI**

<b>Type</b>	125
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	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.
<b>Parent TLV</b>	PHS Rule

1 **5.3.2.126PHSM**

<b>Type</b>	126
<b>Length in octets</b>	Variable
<b>Value</b>	Bit string
<b>Description</b>	<p>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:</p> <ul style="list-style-type: none"> <li>• Bit #0: 0 = Do not suppress first byte of the suppression field, 1 = Suppress first byte of the suppression field.</li> <li>• Bit #1: 0 = Do not suppress second byte of the suppression field, 1 = Suppress second byte of the suppression field.</li> <li>• Bit #x: 0 = Do not suppress (x+1) byte of the suppression field, 1 = Suppress (x+1) byte of the suppression field.</li> </ul>
<b>Parent TLV</b>	PHS Rule

2 **5.3.2.127PHS Rule**

<b>Type</b>	127	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Parameters associated with a PHS Rule. Omission means PHS is disabled.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	PHSI	M
	PHSS	M
	PHSF	M
	PHSM	M
	PHSV	M
	PHS Rule Action	O
<b>Parent TLV</b>	SF Info	

1 **5.3.2.128 PHS Rule Action**

<b>Type</b>	128
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Add PHS Rule</li> <li>• 0x01 = Replace PHS Rule</li> <li>• 0x02 = Delete PHS Rule</li> <li>• 0x03 = Delete All PHS Rules</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	PHS Action Code.
<b>Parent TLV</b>	PHS Rule

2 **5.3.2.129 PHSS**

<b>Type</b>	129
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	<p>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.</p>
<b>Parent TLV</b>	PHS Rule

3 **5.3.2.130 PHSV**

<b>Type</b>	130
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Verify</li> <li>• 0x01 = Don't verify</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	<p>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.</p>
<b>Parent TLV</b>	PHS Rule

1 **5.3.2.131 PPAQ**

<b>Type</b>	131	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	<p>Used for One-Time charging, report usage, the request for further quota and quota delivery. It is also used in order to request prepaid quota for a new service instance or to allocate the (initial and subsequent) quotas.</p> <p>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).</p>	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Quota Identifier	M
	Volume Quota	O
	Volume Threshold	O
	VolumeUsed	O
	Duration Quota	O
	Duration Threshold	O
	Duration Used	O
	Resource Quota	O
	Resource Threshold	O
	Update Reason	O
	Service-ID	O
	Rating-Group-ID	O
	Termination Action	O
	Pool-ID	O
	Pool-Multiplier	O
	Prepaid Server	O
	SFID (one or more)	O <sup>23</sup>
<b>Parent TLV</b>	MS Info	

<sup>23</sup> SF ID(s) shall be included in flow based prepaid accounting scenario.

1 **5.3.2.132 Duration Used**

<b>Type</b>	132
<b>Length in octets</b>	4
<b>Value</b>	Unsigned Integer representing seconds.
<b>Description</b>	This optional TLV is only present if duration-based charging is used. It is encoded as an integer. It indicates the Active time duration (in seconds) since the start of the accounting session related to the QuotaID of the PPAQ in which it occurs.
<b>Parent TLV(s)</b>	PPAQ

2

3 **5.3.2.133 PMK SN**

<b>Type</b>	133
<b>Length in octets</b>	1
<b>Value</b>	0X0000   4-bit PMK SN.
<b>Description</b>	PMK Sequence Number as specified by IEEE 802.16e.
<b>Parent TLV(s)</b>	MS Security History

4 **5.3.2.134 PKM2 Message Code**

<b>Type</b>	134
<b>Length in octets</b>	1
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"> <li>0x0x12 = EAP Transfer</li> </ul> All other values are Reserved.
<b>Description</b>	The value of this parameter indicates to BS the message code that SHOULD be used on PKMv2 and indirectly the state of authentication process.
<b>Parent TLV(s)</b>	Authentication Complete

5 **5.3.2.135 Paging Interval Length**

<b>Type</b>	135
<b>Length in octets</b>	2
<b>Value</b>	Unsigned 32-bit integer
<b>Description</b>	Max duration in frames of Paging Listening interval. Used in calculation of Paging listening interval (aligned with 802.16).
<b>Parent TLV(s)</b>	Paging Information

### 1 5.3.2.136PN Counter

<b>Type</b>	136
<b>Length in octets</b>	4
<b>Value</b>	Unsigned 32-bit integer.
<b>Description</b>	Last value of PN Counter used on DL (for AES CCM cipher suite).
<b>Parent TLV(s)</b>	Older TEK Parameters, Newer TEK Parameters

### 2 5.3.2.137Preamble Index / Sub-channel Index

<b>Type</b>	137
<b>Length in octets</b>	1
<b>Value</b>	Unsigned 8-bit integer.
<b>Description</b>	Represents Preamble Index/Sub-channel Index.
<b>Parent TLV</b>	BS Info, RRM BS Info

### 3 5.3.2.138Protocol

<b>Type</b>	138
<b>Length in octets</b>	1
<b>Value</b>	8 bit integer, representing IP Protocol: protocol.
<b>Description</b>	The value of the field specifies a matching value 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.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

### 4 5.3.2.139Protocol Destination Port Range

<b>Type</b>	139
<b>Length in octets</b>	4
<b>Value</b>	This field is coded as follows: <ul style="list-style-type: none"> <li>• Octet 1 = MSB of DstPortLow</li> <li>• Octet 2 = LSB of DstPortLow</li> <li>• Octet 3 = MSB of DstPortHigh</li> <li>• Octet 4 = LSB of DstPortHigh</li> </ul>
<b>Description</b>	The value of the field specifies a range 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 destination port is irrelevant. This parameter is irrelevant for protocols without port numbers.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

### 5.3.2.140 Protocol Source Port Range

<b>Type</b>	140
<b>Length in octets</b>	4
<b>Value</b>	<p>This field is coded as follows:</p> <ul style="list-style-type: none"> <li>• Octet 1 = MSB of SrcPortLow</li> <li>• Octet 2 = LSB of SrcPortLow</li> <li>• Octet 3 = MSB of SrcPortHigh</li> <li>• Octet 4 = LSB of SrcPortHigh</li> </ul>
<b>Description</b>	<p>The value of the field specifies a range 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.</p>
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

### 5.3.2.141 QoS Parameters

Type	141	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains all Parameters pertaining to a specific QoS Description.	
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
	Media Flow Description in SDP Format	O
	Reduced Resources Code	O <sup>1</sup>
	Data Integrity	O <sup>1</sup>
	DSCP	O
	Parent TLV	SF Info

If no Data Delivery Service Sub-TLV is included then the Data Delivery Service defaults to BE Data Delivery Service with Traffic Priority equal to zero and Request Transmit Policy equal to zero.

Notes:

1. TLV is not applicable to MCBSC Service.



1 **5.3.2.142 Radio Resource Fluctuation**

<b>Type</b>	142
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	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."
<b>Parent TLV(s)</b>	RRM BS Info

2 **5.3.2.143 Void**

3 **5.3.2.144 REG Context**

<b>Type</b>	144	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	MS REG context parameters that has been agreed between MS and BS and delivered in REG-RSP message during the initial network entry of MS.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Number of UL Transport CIDs Support	M
	Number of DL Transport CIDs Support	M
	Classification/PHS Options and SDU Encapsulation Support	O <sup>24</sup>
	Maximum Number of Classifier	O <sup>24</sup>
	PHS Support	O <sup>24</sup>
	ARQ Support	M
	DSx Flow Control	O <sup>24</sup>
	Total Number of Provisioned Service Flows	O
	Maximum MAC Data per Frame Support	O <sup>24</sup>
	Packing Support	M
	MAC ertPS Support	O <sup>24</sup>
	Maximum Number of Bursts Transmitted Concurrently to the MS	M
	HO Supported	M
	HO Process Optimization MS Timer	M
	Mobility Features Supported	M
	Sleep Mode Recovery Time	M

<sup>24</sup> This TLV may be omitted when its default value is to be used

	Idle Mode Timeout	O <sup>24</sup>
	ARQ Ack Type	O <sup>24</sup>
	MS HO Connections Parameters Proc Time	M
	MS HO TEK Proc Time	M
	MAC Header and Extended Sub-Header Support	M
	System Resource Retain Timer	O
	MS Handover Retransmission Timer	O
	Handover Indication Readiness Timer	M
	BS Switching Timer	M
	Power Saving Class Capability	M
<b>Parent TLV(s)</b>	MS Info	

1 **5.3.2.145 Registration Type**

<b>Type</b>	145
<b>Length in octets</b>	4
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00000000 – Initial Network Entry</li> <li>• 0x00000001 – Handoff</li> <li>• 0x00000002 – In-Service Data Path Establishment</li> <li>• 0x00000003 – MS Network Exit</li> <li>• 0x00000004 – Idle Mode Entry</li> <li>• 0x00000005 – Idle Mode Exit</li> <li>• 0x00000006 – Anchor DPF Relocation</li> <li>• 0x00000007 – In-Service Data Path De-Registration</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indication of the process which includes data path (Pre-) Registration.
<b>Message Primitives That Use This TLV</b>	DP Control messages (Path (Pre-/De-) Registration/Modification Request/Response/Acknowledge), HO_Req

2 **5.3.2.146 Relative Delay**

<b>Type</b>	146
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Represents the Target BS Relative Delay in milliseconds.
<b>Parent TLV</b>	BS Info

1 **5.3.2.147 Registration Lifetime**

<b>Type</b>	147
<b>Length in octets</b>	2
<b>Value</b>	Registration Lifetime as defined in RFC 3344.
<b>Description</b>	The remaining lifetime (measured in seconds).
<b>Parent TLV</b>	MIP4 Info

2 **5.3.2.148 Quota Identifier**

<b>Type</b>	148
<b>Length in octets</b>	4
<b>Value</b>	Octet String. The Quota Identifier value (most significant bit first).
<b>Description</b>	Quota Identifier.
<b>Parent TLV(s)</b>	PPAQ

3 **5.3.2.149 Relocation Success Indicator**

<b>Type</b>	149
<b>Length in octets</b>	1
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"><li>• 0x00 = Accept</li><li>• 0x01 = Refuse</li></ul> All other values are Reserved.
<b>Description</b>	Indicates confirmation of whether the Relocation was accepted and completed by the Relocation Destination.
<b>Parent TLV(s)</b>	Paging Information

1 **5.3.2.150 Request/Transmission Policy**

<b>Type</b>	150
<b>Length in octets</b>	4
<b>Value</b>	<p>32-bit bitmask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 = Service flow SHALL not use broadcast bandwidth request opportunities. (Uplink only).</li> <li>• Bit #1 –Service flow SHALL NOT use multicast bandwidth request opportunities. (Uplink only).</li> <li>• Bit #2 = Service flow SHALL not piggyback requests with data. (Uplink only).</li> <li>• Bit #3 = Service flow SHALL not fragment data.</li> <li>• Bit #4 = Service flow SHALL not suppress payload headers (CS parameter).</li> </ul> <p>[Note that the following description is an excerption from [13].]</p> <p>If bit #4 is set to '0' and both the SS and the BS support PHS (according to section 11.7.7.3 of IEEE std 802.16), each SDU for this service flow SHALL be prefixed by a PHSI field, which may be set to 0 (see section 5.2). If bit #4 is set to '1', none of the SDUs for this service flow will have a PHSI field.</p> <ul style="list-style-type: none"> <li>• Bit #5 = Service flow SHALL not pack multiple SDUs (or fragments) into single MAC PDUs.</li> <li>• Bit #6 = Service flow SHALL not include CRC in the MAC PDU.</li> <li>• Bit #7 = The service flow SHALL NOT compress payload headers using ROHC.</li> </ul> <p>[Note that the following description is an excerption from [13].]</p> <p>If bit #7 is set to '0' and both the SS and the BS support ROHC (according to section 11.7.7.4 of IEEE std 802.16), each SDU for this service flow SHALL be compressed using ROHC. If bit 7 is set to '1', none of the SDUs SHALL be compressed.</p> <p>All other bits are Reserved.</p>
<b>Description</b>	<p>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.</p>
<b>Parent TLV</b>	<p>BE Data Delivery Service, ERT-VR Data Delivery Service, NRT-VR Data Delivery Service, RT-VR Data Delivery Service, UGS Data Delivery Service</p>

### 1 5.3.2.151 Reservation Action

<b>Type</b>	151
<b>Length in octets</b>	2
<b>Value</b>	<p>The Action field is a 16 bit vector with the following meaning for each bit being set to “1”:</p> <ul style="list-style-type: none"> <li>• Bit 15 (0x0001) = Create service flow</li> <li>• Bit 14 (0x0002) = Admit service flow</li> <li>• Bit 13 (0x0004) = Activate service flow</li> <li>• Bit 12 (0x0008) = Modify service flow</li> <li>• Bit 11 (0x0010) = Delete service flow</li> <li>• Bits 0 – 10 = Undefined</li> </ul> <p>All other bits are Reserved.</p>
<b>Description</b>	<p>Identifies the requested resource reservation action.</p> <p>More than one of bits #13-#15 MAY be set to 1 at the same time (for instance, create &amp; admit, or create/admit/activate/ modify a service flow).</p>
<b>Parent TLV</b>	SF Info

### 2 5.3.2.152 Reservation Result

<b>Type</b>	152
<b>Length in octets</b>	2
<b>Value</b>	<p>Result can be one of the following:</p> <ul style="list-style-type: none"> <li>• 0x0000 = Successfully Created</li> <li>• 0x0001 = Request Denied – No resources</li> <li>• 0x0002 = Request Denied due to Policy</li> <li>• 0x0003 = Request Denied due to Requests for Other Flows Failed</li> <li>• 0x0004 = Request Failed (Unspecified reason)</li> <li>• 0x0005 = Request Denied due to MS reason</li> <li>• Values in the range 0x0006 – 0xFEFF are Reserved</li> <li>• Values in the range 0xFF00 – 0xFFFF are Reserved</li> </ul>
<b>Description</b>	Indicates the result of a Resource Reservation Request.
<b>Parent TLV</b>	SF Info

### 1 5.3.2.153 Response Code

<b>Type</b>	153
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Not allowed - Paging Reference is zero</li> <li>• 0x01 = Not allowed - No such SF</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates reason for not paging the MS.
<b>Message Primitives that Use This TLV</b>	Initiated_Paging_Rsp

### 2 5.3.2.154 Result Code

<b>Type</b>	154
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Success</li> <li>• 0x01 = Failure – No resources</li> <li>• 0x02 = Failure – Not supported</li> <li>• 0x03 = Partial Response</li> <li>• 0x04 = Multiple Not Supported</li> <li>• 0x05 = Request Failure</li> <li>• The values in the range 0x06 – 0x99 are Reserved</li> <li>• The values in the range 0xA0 – 0xFF are Reserved</li> </ul>
<b>Description</b>	Indicates if the requested action was successfully supported at the intended target.
<b>Message Primitives that use this TLV</b>	HO related messages, Path (pre-)registration and context related messages.

### 3 5.3.2.155 Void

### 4 5.3.2.156 Round Trip Delay

<b>Type</b>	156
<b>Length in octets</b>	1
<b>Value</b>	8-bit integer representing Serving BS Round Trip Delay in the units of 1/Fs.
<b>Description</b>	
<b>Parent TLV</b>	BS Info

1 **5.3.2.157RRM Absolute Threshold Value J**

<b>Type</b>	157
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = 0%</li> <li>• 0x01 = 1%</li> <li>• ...</li> <li>• 0x64 = 100%</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	The threshold value J is used by BS (RRA) as the absolute threshold for reporting.
<b>Message Primitives That Use This TLV</b>	RRM <i>Spare_Capacity_Req</i> , RRM <i>Spare_Capacity_Rpt</i> .

2 **5.3.2.158RRM Averaging Time T**

<b>Type</b>	158
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer, in units of 100 msec.
<b>Description</b>	Used by BS (RRA) as the measurement interval for producing the information requested by RRC.
<b>Message Primitives That Use This TLV</b>	RRM <i>Spare_Capacity_Req</i> , RRM <i>Spare_Capacity_Rpt</i> .

1 **5.3.2.159RRM BS Info**

<b>Type</b>	159	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Contains a description of BS parameters which are not related to a specific MS.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	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
	DCD Setting	O
	UCD Setting	O
	Full DCD Setting	O
	Full UCD Setting	O
	HO Process Optimization	O
	Preamble Index / Sub-channel Index	O
	Mobility Features Supported	O
	PHY Mode ID	O
	Scheduling Service Supported	O
<b>Message Primitives That Use This TLV</b>	RRM <i>Spare_Capacity_Rpt</i> , RRM <i>Neighbor_BS_Resource_Status_Update</i> , RRM <i>Radio_Config_Update_Rpt</i> .	



1 **5.3.2.160 RRM BS-MS PHY Quality Info**

<b>Type</b>	160	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	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.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	BS ID	M
	Serving/Target Indicator	O
	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
	Preamble Index / Sub-channel Index	O
	SF Info (for Data Integrity)	O
<b>Message Primitives That Use This TLV</b>	RRM PHY_Parameters_Rpt	

2 **5.3.2.161 RRM Relative Threshold RT**

<b>Type</b>	161	
<b>Length in octets</b>	1	
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = 0%</li> <li>• 0x01 = 1%</li> <li>• ...</li> <li>• 0x64 = 100%</li> </ul> <p>All other values are Reserved.</p>	
<b>Description</b>	The threshold value RT is used by BS (RRA) to keep track of the threshold from the last measurement period.	
<b>Message Primitives That Use This TLV</b>	RRM <i>Spare_Capacity_Req</i> , RRM <i>Spare_Capacity_Rpt</i> .	

### 1 5.3.2.162 RRM Reporting Characteristics

<b>Type</b>	162
<b>Length in octets</b>	4
<b>Value</b>	32-bit bitmask with the following values. <ul style="list-style-type: none"> <li>• Bit #0 = periodically as defined by reporting period P</li> <li>• Bit #1 = regularly whenever resources have changed as defined by RT since the last measurement period.</li> <li>• Bit #2 = regularly whenever resources cross predefined total threshold(s) defined by reporting absolute threshold values J</li> <li>• Bit #3 = DCD/UCD Configuration Change Count modification</li> <li>• All Bit = 0 means “Stop RRM Reporting”, if the TLV is in the Request message, and “RRM Reporting Stopped”, if the TLV is in the Report Message.</li> </ul> All other bits are Reserved.
<b>Description</b>	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified.
<b>Message Primitives That Use This TLV</b>	RRM <i>Spare_Capacity_Req</i> , RRM <i>Spare_Capacity_Rpt</i> .

### 2 5.3.2.163 RRM Reporting Period P

<b>Type</b>	163
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer, in units of 100 msec.
<b>Description</b>	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.
<b>Message Primitives That Use This TLV</b>	RRM <i>Spare_Capacity_Req</i> , RRM <i>Spare_Capacity_Rpt</i> .

### 3 5.3.2.164 RRM Spare Capacity Report Type

<b>Type</b>	164
<b>Length in octets</b>	1
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"> <li>• 0x00 = “Type 1” which refers to reporting of the “Available radio resource indicator”</li> </ul> All other values are Reserved.
<b>Description</b>	The value of this parameter specifies the type of RRM <i>Spare_Capacity_Rpt</i> Forward compatibility.
<b>Message Primitives That Use This TLV</b>	RRM <i>Spare_Capacity_Req</i> , RRM <i>Spare_Capacity_Rpt</i> .

1 **5.3.2.165 RT-VR Data Delivery Service**

<b>Type</b>	165	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	This compound TLV contains the QoS parameters relevant for RT-VR Data Delivery Service. If included in QoS Parameters, it implies rtPS Scheduling Service for UL connections.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	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
<b>Parent TLV</b>	QoS Parameters	

2 Note [a]: Used during Service flow creation, HO/ Idle Mode entry/exit operations.

3 **5.3.2.166 RxPN Counter**

<b>Type</b>	166
<b>Length in octets</b>	4
<b>Value</b>	Unsigned 32-bit integer.
<b>Description</b>	Last value of PN Counter used on UL (for AES CCM cipher suite).
<b>Parent TLV(s)</b>	Older TEK Parameters, Newer TEK Parameters

4 **5.3.2.167 Volume Quota**

<b>Type</b>	167
<b>Length in octets</b>	4
<b>Value</b>	The attribute is an unsigned Integer representing a volume measured in kilo-bytes (1024 bytes).
<b>Description</b>	Indicates the volume (in octets) allocated for the session or the total used volume (in octets) for both inbound and outbound traffic.
<b>Parent TLV(s)</b>	PPAQ

5 **5.3.2.168 Volume Threshold**

<b>Type</b>	168
<b>Length in octets</b>	4

<b>Value</b>	The attribute is an unsigned Integer representing a volume measured in kilo-bytes (1024 bytes).
<b>Description</b>	This TLV is optionally present if Volume Quota is present. It indicates the volume (in octets) that SHALL be consumed before a new quota should be requested. This threshold should not be larger than the Volume Quota.
<b>Parent TLV(s)</b>	PPAQ

1 **5.3.2.169 SAID**

<b>Type</b>	169
<b>Length in octets</b>	2
<b>Value</b>	SAID definition as per 802.16.
<b>Description</b>	The SAID is a 16-bit identifier for the SA.
<b>Parent TLV(s)</b>	SF Info, SA Descriptor

2 **5.3.2.170 SA Descriptor**

<b>Type</b>	170	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>	Set of SA-related IEs.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	SAID	M
	SA Type	M
	SA Service Type	O
	Cryptographic Suite	M
	Older TEK Parameters	O
	Newer TEK Parameters	O
<b>Parent TLVs</b>	MS Info	

3 **5.3.2.171 Certified-MS-Feature-List-For-GW**

<b>Type</b>	171	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>		
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Certified-For-MCBCS	O
	Certified-For-LBS	O
	Certified-For-Compression	O
<b>Parent TLVs</b>	MS Authorization Context	

1 **5.3.2.172 SA Service Type**

<b>Type</b>	172
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Unicast Service</li> <li>• 0x01 = Group Multicast Service</li> <li>• 0x02 = MBS Service</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	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.
<b>Parent TLV(s)</b>	SA Descriptor

2 **5.3.2.173 SA Type**

<b>Type</b>	173
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Primary</li> <li>• 0x01 = Static</li> <li>• 0x02 = Dynamic</li> </ul> <p>All values in the range 0x80 – 0xFF are Vendor Specific.</p> <p>All other values are Reserved.</p>
<b>Description</b>	Type of SA.
<b>Parent TLV(s)</b>	SA Descriptor

3 **5.3.2.174 SBC Context**

<b>Type</b>	174	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	MS SBC context parameters that has been agreed between MS and BS and delivered in SBC-RSP message during the initial network entry of MS.	
<b>Elements</b>	<b>TLV Name</b>	<b>M/O</b>
	Subscriber Transition Gaps	M
	Maximum Transmit Power	M
	Capabilities for Construction and Transmission of MAC PDUs	M
	PKM Flow Control	O <sup>24</sup>
	Maximum Number of Supported Security Associations	O <sup>24</sup>
	Security Negotiation Parameters	M

	Extended Subheader Capability	M
	HO Trigger Metric Support	M
	Current Transmit Power	M
	OFDMA SS FFT Sizes	M
	OFDMA SS demodulator	M
	OFDMA SS modulator	M
	The number of UL HARQ Channel	M
	OFDMA SS Permutation support	M
	OFDMA SS CINR Measurement Capability	M
	The number of DL HARQ Channels	M
	HARQ Chase Combining and CC-IR Buffer Capability	M
	OFDMA SS Uplink Power Control Support	M
	OFDMA SS Uplink Power Control Scheme Switching Delay	M
	OFDMA MAP Capability	M
	Uplink Control Channel Support	M
	OFDMA MS CSIT Capability	M
	Maximum Number of Burst per Frame Capability in HARQ	O <sup>24</sup>
	OFDMA SS demodulator for MIMO Support	M
	OFDMA SS modulator for MIMO Support	M
	OFDMA Parameters Sets	O <sup>25</sup>
<b>Parent TLV(s)</b>	MS Info	

### 1 5.3.2.175SDU BSN Map

<b>Type</b>	175
<b>Length in octets</b>	Variable
<b>Value</b>	Bitmap expressing which Blocks of the SDU have been transmitted and/or acknowledged.
<b>Description</b>	
<b>Parent TLV</b>	SDU Info

### 2 5.3.2.176SDU Info

Type	176		
Length in octets	Variable		
Value			
Description	Information about an SDU involved in Data Path Integrity operations.		
Elements (Sub-	TLV Name		M/O

<sup>25</sup> All TLVs must be present except if the "OFDMA parameters sets" TLV is present.

<b>TLVs)</b>	SDU SN	M
	SDU BSN Map	O
	Pointer BSN	O
<b>Parent TLV</b>	SF Info	

1 **5.3.2.177 SDU Size**

<b>Type</b>	177
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer. Default = 49.
<b>Description</b>	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).
<b>Parent TLV</b>	UGS Data Delivery Service

2 **5.3.2.178 SDU SN**

<b>Type</b>	178
<b>Length in octets</b>	4
<b>Value</b>	SDU Sequence Number (for Data Path Integrity operations).
<b>Description</b>	
<b>Parent TLV</b>	SDU Info

3 **5.3.2.179 Service Class Name**

<b>Type</b>	179
<b>Length in octets</b>	2 – 128
<b>Value</b>	Service Class Name as defined in IEEE802.16e.
<b>Description</b>	ASCII string, which is known at the BS and which indirectly specifies a set of QoS Parameters.
<b>Parent TLV</b>	QoS Parameters R3 QoS Descriptor

4 **5.3.2.180 Service Level Prediction**

<b>Type</b>	180
<b>Length in octets</b>	1
<b>Value</b>	8-bit integer representing Service Level Prediction.
<b>Description</b>	
<b>Parent TLV</b>	BS Info

1 **5.3.2.181 Service Authorization Code**

<b>Type</b>	181
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Service authorized</li> <li>• 0x01 = Service not authorized</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Code indicating whether or not service is authorized.
<b>Parent TLV</b>	MS Info

2 **5.3.2.182 Serving/Target Indicator**

<b>Type</b>	182
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Serving</li> <li>• 0x01 = Target</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates if the designated BS is the Serving BS or Target BS for the handover.
<b>Message Primitives That Use This TLV</b>	HO related messages.
<b>Parent TLV(s)</b>	BS Info, RRM BS_MS PHY Quality Info

3 **5.3.2.183 Certified-MS-Feature-List-For-BS**

<b>Type</b>	183	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>		
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Certified-For-Scan-Capability	O
	Certified-For-Security-Capability	O
	Certified-For-ARQ-Capability	O
<b>Parent TLVs</b>	MS Authorization Context	



1 **5.3.2.184 SFID**

<b>Type</b>	184
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	SFID definition as per 802.16.
<b>Parent TLV(s)</b>	SF Info

2 **5.3.2.185 SF Info**

<b>Type</b>	185	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Service Flow Description.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Failure Indication Details	O <sup>1</sup>
	SFID	M
	Reservation Action	O <sup>1</sup>
	Reservation Result	O <sup>1</sup>
	HARQ Context	O
	ARQ Enable	O <sup>1</sup>
	ARQ Context	O <sup>1</sup>
	Direction	O <sup>1</sup>
	CID/MCID	O <sup>2</sup>
	SAID	O <sup>1</sup>
	Packet Classification Rule / Media Flow Description (one or more)	O
	QoS Parameters	O
	VLANTagProcessingRuleID	O
	Paging Preference	O <sup>1</sup>
	CS Type	O
	Data Integrity Method	O
	Data Path Info	O
	SDU Info	O <sup>1</sup>
	PHS Rule	O <sup>1</sup>
	Accounting Extension	O
	SA Descriptor	O <sup>1</sup>
	Correlation ID	O
	Data Delivery Trigger	O

	Pointer BSN	O
	BSN ARQ State Bitmap	O <sup>1</sup>
	MCBCS Service continuity indicator	O <sup>3</sup>
	MBS Zone ID	O <sup>3</sup>
	MCBCS Transmission Zone ID	O <sup>3,4</sup>
	PDFID	O <sup>3,4</sup>
	Data Integrity Applied	O
<b>Parent TLV(s)</b>	MS Info, BS Info	

Note: Multiple instances of SF Info may be included in one message

Notes:

1. TLV is not applicable for MCBCS Service
2. MCID is used in case of MCBCS Service
3. TLV is only applicable for MCBCS Service
4. PDFID SHALL be used together with MCBCS Transmission Zone to uniquely identify a service flow of MBS with MCBCS Transmission Zone.

#### 5.3.2.186 Spare Capacity Indicator

<b>Type</b>	186
<b>Length in octets</b>	2
<b>Value</b>	16-bit signed integer.
<b>Description</b>	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.
<b>Parent TLV</b>	BS Info

#### 5.3.2.187 TEK

<b>Type</b>	187
<b>Length in octets</b>	Two fixed sizes, either 8 or 16
<b>Value</b>	64-bit or 128-bit string.
<b>Description</b>	Traffic Encryption Key.
<b>Parent TLV(s)</b>	Older TEK Parameters, Newer TEK Parameters

1 **5.3.2.188 TEK Lifetime**

<b>Type</b>	188
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	The remaining TEK Lifetime in seconds. The value 0x00000000 means that the corresponding TEK is not valid.
<b>Parent TLV(s)</b>	Older TEK Parameters, Newer TEK Parameters

2 **5.3.2.189 TEK SN**

<b>Type</b>	189
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = TEK Sequence Number 0</li> <li>• 0x01 = TEK Sequence Number 1</li> <li>• 0x02 = TEK Sequence Number 2</li> <li>• 0x03 = TEK Sequence Number 3</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	2-bit TEK Sequence Number.
<b>Parent TLV(s)</b>	Older TEK Parameters, Newer TEK Parameters

3 **5.3.2.190 Tolerated Jitter**

<b>Type</b>	190
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer (in milliseconds).
<b>Description</b>	This parameter represents the maximum delay variation (jitter) (in milliseconds).
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>• UGS Data Delivery Service</li> <li>• ERT-VR Data Delivery Service</li> <li>• R3 QoS Descriptor</li> </ul>

4 **5.3.2.191 Total Slots DL**

<b>Type</b>	191
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	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.
<b>Parent TLV(s)</b>	RRM BS Info

5 **5.3.2.192 Total Slots UL**

<b>Type</b>	192
-------------	-----

<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	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.
<b>Parent TLV(s)</b>	RRM BS Info

### 1 5.3.2.193 Traffic Priority

<b>Type</b>	193
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Priority 0</li> <li>• 0x01 = Priority 1</li> <li>• 0x02 = Priority 2</li> <li>• 0x03 = Priority 3</li> <li>• 0x04 = Priority 4</li> <li>• 0x05 = Priority 5</li> <li>• 0x06 = Priority 6</li> <li>• 0x07 = Priority 7</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	<p>The value of this parameter specifies the priority assigned to a service flow as it is defined for the Traffic Priority in IEEE802.16e [11]. 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. Higher numbers indicate higher priority. Default 0.</p>
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>• BE Data Delivery Service</li> <li>• UGS Data Delivery Service</li> <li>• NRT-VR Data Delivery Service</li> <li>• RT-VR Data Delivery Service</li> <li>• ERT-VR Data Delivery Service</li> <li>• R3 QoS Descriptor</li> </ul>

1 **5.3.2.194 Tunnel Endpoint**

<b>Type</b>	194
<b>Length in octets</b>	Variable (either 4 or 16 octets)
<b>Value</b>	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.
<b>Description</b>	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.
<b>Parent TLV(s)</b>	Data Path Info

2 **5.3.2.195 UCD Setting**

<b>Type</b>	195
<b>Length in octets</b>	Variable
<b>Value</b>	Compound, as specified in [802.16e-2005], section 11.1.7.
<b>Description</b>	<p>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.</p> <p>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.</p> <p>See [802.16e-2005], section 11.1.7.</p>
<b>Parent TLV(s)</b>	RRM BS Info

3 **5.3.2.196 UGS Data Delivery Service**

<b>Type</b>	196	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	This compound TLV contains the QoS parameters relevant for UGS Data Delivery Service. If included in QoS Parameters, it implies UGS Scheduling Service for UL connections.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O Flag</b>
	Minimum Reserved Traffic Rate	O
	Maximum Sustained 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])
<b>Parent TLV</b>	QoS Parameters	

1 Note [a]: Used during Service flow creation, HO/ Idle Mode entry/exit operations.

## 2 5.3.2.197 UL PHY Quality Info

<b>Type</b>	197
<b>Length in octets</b>	4
<b>Value</b>	<ul style="list-style-type: none"> <li>Octet 1: 8-bit UL RSSI Mean</li> <li>Octet 2: 8-bit UL RSSI Std</li> <li>Octet 3: 8-bit UL CINR Mean</li> <li>Octet 4: 8-bit UL CINR Std</li> </ul>
<b>Description</b>	
<b>Parent TLV</b>	BS Info

## 3 5.3.2.198 UL PHY Service Level

<b>Type</b>	198
<b>Length in octets</b>	4
<b>Value</b>	32-bit integer representing UL PSL.
<b>Description</b>	
<b>Parent TLV</b>	BS Info

## 4 5.3.2.199 Unsolicited Grant Interval

<b>Type</b>	199
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer representing the grant interval (in milliseconds).
<b>Description</b>	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).
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>ERT-VR Data Delivery Service</li> <li>UGS Data Delivery Service</li> <li>R3 QoS Descriptor</li> </ul>

## 5 5.3.2.200 Unsolicited Polling Interval

<b>Type</b>	199
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer representing the polling interval (in milliseconds).
<b>Description</b>	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
<b>Parent TLV</b>	RT-VR Data Delivery Service

1

2 **5.3.2.201 VAAA IP Address**

<b>Type</b>	201
<b>Length in octets</b>	Variable (either 4 or 16)
<b>Value</b>	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.
<b>Description</b>	VAAA IPv4 or IPv6 address.
<b>Parent TLV(s)</b>	MS Security History

3 **5.3.2.202 VAAA Realm**

<b>Type</b>	202
<b>Length in octets</b>	Variable up to 256 octets
<b>Value</b>	ASCII String
<b>Description</b>	VAAA realm character string.
<b>Parent TLV(s)</b>	MS Security History

4 **5.3.2.203 BS HO RSP Code**

<b>Type</b>	203
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Void</li> <li>• 0x01 = Target BS doesn't support this HO Type</li> <li>• 0x02 = Target BS's air link resource is not enough</li> <li>• 0x03 = Target BS's CPU overload</li> <li>• 0x04 = Target BS rejects for other reasons</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	This TLV is used to carry HO failure reason for target BS.
<b>Parent TLV(s)</b>	BS Info

1 **5.3.2.204 Accounting Context**

<b>Type</b>	204	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Accounting Context.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Accounting Mode Provisioning	M
	R3 Acct Session Time	O <sup>1</sup>
	R3 Active Time	O <sup>1</sup>
	Interim Update Interval Remaining	O <sup>2</sup>
<b>Message Primitives That Use This TLV</b>	RR_Req (Create) / HO_Req/Context_Rpt / Relocation_Complete_Rsp/Anchor_DPF_HO_Req Anchor_DPF_HO_Trigger	

2 <sup>1</sup> These sub-TLVs are only included in the Relocation\_Complete\_Rsp message

3 <sup>2</sup> This sub-TLV is only included in the Anchor\_DPF\_HO\_Req message

4 **5.3.2.205 HO ID**

<b>Type</b>	205
<b>Length in octets</b>	Shall follow 802.16e
<b>Value</b>	
<b>Description</b>	This IE is defined in the IEEE 802.16e spec.
<b>Parent TLV(s)</b>	BS Info

5 **5.3.2.206 Combined Resource Indicator**

<b>Type</b>	206
<b>Length in octets</b>	3
<b>Value</b>	Compound



<b>Description</b>	<p>This TLV indicates whether or not pre-provisioned service flows for the indicated CS type must be successfully established in order for the indicated CS type to remain active at the ASN.</p> <p>The TLV can be applied per MS or per CS type. If the CS Type TLV indicates “All CS Types”, then the Combines Resource Required TLV is applied for the MS. In this usage, there can be only a single instance of this TLV. If the CS Type TLV indicates a specific CS type, the TLV is applied for the indicated CS. In this usage, there can be multiple instances of this TLV if the indicated CS types can be supported concurrently according to this specification.</p> <p>If the CS Type indicates “All CS Types”, and the Combined Resources Required TLV indicates “combined”, then all pre-provisioned SFs for the MS are required to be successfully established in order for the MS to remain active at the ASN. If the Combined Resources Required TLV indicates “not combined”, then there is no restriction on the independent establishment of any pre-provisioned SFs.</p> <p>If the CS Type indicates a specific CS Type, and the Combined Resources Required TLV indicates “combined”, then all of the pre-provisioned SFs for the indicated CS type are required to be successfully established for the indicated CS type to remain active at the ASN. If the Combined Resources Required TLV indicates “not combined”, then there is no restriction on the independent establishment of pre-provisioned SFs for the indicated CS type.</p> <p>Separate QoS resource reservation messages may be sent for each group of service flows indicated by the combined resource indicator.</p>	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	CS Type	M
	Combined Resources Required	M
<b>Parent TLV(s)</b>	MS Info	

1 **5.3.2.207 R3 WiMAX Capability**

<b>Type</b>	207	
<b>Length</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>		
<b>Elements</b>	<b>TLV Name</b>	<b>M/O</b>
	R3 WiMAX-Release	M
	R3 Accounting Capabilities	M
	R3 Hotlining Capability	O
	R3 Idle Notification Capabilities	O
<b>Parent TLV</b>	Ms Authorization Context	

### 1 5.3.2.208R3 Accounting Capabilities

<b>Type</b>	208
<b>Length</b>	1
<b>Value</b>	1 octet Bit Mask with the following values: <ul style="list-style-type: none"> <li>• 0x00 = No accounting. Only valid at the HA</li> <li>• 0x01 = Session-based accounting. Default value for the ASN</li> <li>• 0x02 = Flow-based accounting for IP-CS</li> <li>• 0x04 = Flow-based accounting for ETH-CS</li> <li>• The rest of the bits are reserved.</li> </ul>
<b>Description</b>	Accounting Capabilities.
<b>Parent TLV</b>	R3 WiMAX Capability

### 2 5.3.2.209R3 Idle Notification Capabilities

<b>Type</b>	209
<b>Length</b>	1
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"> <li>• 0x00 = Idle Mode notification is not supported or is not required</li> <li>• 0x01 = Idle Mode notification is supported and is required</li> </ul> All other values are Reserved.
<b>Description</b>	Idle notification Capabilities.
<b>Parent TLV</b>	R3 WiMAX Capability

### 3 5.3.2.210R3 CUI

<b>Type</b>	210
<b>Length</b>	Variable
<b>Value</b>	String
<b>Description</b>	CUI
<b>Parent TLV</b>	Ms Authorization Context

### 4 5.3.2.211R3 Class

<b>Type</b>	211
<b>Length</b>	Variable
<b>Value</b>	String
<b>Description</b>	Class
<b>Parent TLV</b>	Ms Authorization Context

### 5 5.3.2.212R3 Framed IP Address

<b>Type</b>	212
-------------	-----

<b>Length</b>	4
<b>Value</b>	32-bits unsigned integer.
<b>Description</b>	Framed-IP-Address.
<b>Parent TLV</b>	Ms Authorization Context

1 **5.3.2.213R3 Framed-IPv6-Prefix**

<b>Type</b>	213
<b>Length</b>	Variable
<b>Value</b>	0-16 bytes.
<b>Description</b>	Framed-IPv6-Prefix.
<b>Parent TLV</b>	Ms Authorization Context

2 **5.3.2.214R3 WiMAX Session ID**

<b>Type</b>	214
<b>Length</b>	Variable
<b>Value</b>	String
<b>Description</b>	WiMAX Session ID.
<b>Parent TLV</b>	Ms Authorization Context

3 **5.3.2.215R3 Packet Flow Descriptor**

<b>Type</b>	215	
<b>Length</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	This TLV is used to carry Packet Flow Descriptor V2 information received over R3.	
<b>Elements</b>	<b>TLV Name</b>	<b>M/O</b>
	SFID	M
	R3 Packet Data Flow ID	M
	R3 Service Data Flow ID	O
	R3 Service Profile ID	O
	R3 Direction	O
	R3 Activation Trigger	O
	R3 Transport Type	O
	R3 Uplink QoS ID	O
	R3 Downlink QoS ID	O
	R3 Uplink Classifier (This TLV is deprecated in this release)	O <sup>26</sup>

<sup>26</sup> This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 only SHALL be used in this Release

	R3 Downlink Classifier (This TLV is deprecated in this release)	O <sup>27</sup>
	R3 Paging Preference	O
<b>Parent TLV</b>	Ms Authorization Context	

1 **5.3.2.216 R3 Packet Data Flow ID**

<b>Type</b>	216
<b>Length</b>	2
<b>Value</b>	Unsigned Short representing the flow identifier (most significant bit first). A value of zero(0) is invalid.
<b>Description</b>	Packet data flow ID.
<b>Parent TLV</b>	R3 Packet-Flow Descriptor

2 **5.3.2.217 R3 Service Data Flow ID**

<b>Type</b>	217
<b>Length</b>	2
<b>Value</b>	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.
<b>Description</b>	Service data flow ID.
<b>Parent TLV</b>	R3 Packet-Flow Descriptor

3 **5.3.2.218 R3 Service Profile ID**

<b>Type</b>	218
<b>Length</b>	4
<b>Value</b>	Unsigned Integer representing the identity of a Flow Spec that is pre-provisioned (most significant bit first). A value of zero(0) is invalid.
<b>Description</b>	Service Profile ID.
<b>Parent TLV</b>	R3 Packet-Flow Descriptor

---

<sup>27</sup> This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 only SHALL be used in this Release

1 **5.3.2.219 R3 Direction**

<b>Type</b>	219
<b>Length</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Reserved</li> <li>• 0x01 = Uplink</li> <li>• 0x02 = Downlink</li> <li>• 0x03 = Bi-directional</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Direction.
<b>Parent TLV</b>	R3 Packet-Flow Descriptor

2 **5.3.2.220 R3 Activation Trigger**

<b>Type</b>	220
<b>Length</b>	1
<b>Value</b>	<ul style="list-style-type: none"> <li>• 0x00 = Reserved</li> <li>• 0x01 = Provisioned (SHALL be set in case of ISF)</li> <li>• 0x02 = Admit (SHALL be set in case of ISF)</li> <li>• 0x04 = Activate (SHALL be set in case of ISF)</li> <li>• 0x08 = Dynamically Reservation (not valid for ISF)</li> </ul> <p>0x10 to 0x80 = Reserved.</p>
<b>Description</b>	Activation Trigger.
<b>Parent TLV</b>	R3 Packet-Flow Descriptor

3 **5.3.2.221 R3 Transport Type**

<b>Type</b>	221
<b>Length</b>	1
<b>Value</b>	<ul style="list-style-type: none"> <li>• 0x00 = Reserved</li> <li>• 0x01 = IPv4-CS</li> <li>• 0x02 = IPv6-CS</li> <li>• 0x03 = Ethernet</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Transport Type.
<b>Parent TLV</b>	R3 Packet-Flow Descriptor

1 **5.3.2.222R3 Uplink QoS ID**

<b>Type</b>	222
<b>Length</b>	1
<b>Value</b>	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.
<b>Description</b>	Uplink QoS ID.
<b>Parent TLV</b>	R3 Packet-Flow Descriptor

2 **5.3.2.223R3 Downlink QoS ID**

<b>Type</b>	223
<b>Length</b>	1
<b>Value</b>	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.
<b>Description</b>	Downlink QoS ID.
<b>Parent TLV</b>	R3 Packet-Flow Descriptor

3 **5.3.2.224R3 Uplink Classifier (This TLV is deprecated in this release)<sup>28</sup>**

4 **5.3.2.225R3 Downlink Classifier (This TLV is deprecated in this release)<sup>29</sup>**

5 **5.3.2.226R3 QoS Descriptor**

<b>Type</b>	226	
<b>Length</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>		
<b>Elements</b>	<b>TLV Name</b>	<b>M/O</b>
	R3 QoS ID	M
	Global Service Class Name	O
	Service Class Name	O
	R3 Schedule Type	M
	Traffic Priority	O
	Maximum Sustained Traffic Rate	O
	Minimum Reserved Traffic Rate	O
	Maximum Traffic Burst	O
	Tolerated Jitter	O
	R3 Maximum Latency	O
	Reduced Resources Code	O

<sup>28</sup> This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 SHALL be used in this Release

<sup>29</sup> This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 SHALL be used in this Release

	R3 Media Flow Type	O
	Unsolicited Grant Interval	O
	R3 SDU Size	O
	R3 Unsolicited Polling Interval	O
	R3 Media Flow Description in SDP Format	O
<b>Parent TLV</b>	Ms Authorization Context	

1 **5.3.2.227 R3 QoS ID**

<b>Type</b>	227
<b>Length</b>	1
<b>Value</b>	Unsigned Octet representing an ID.
<b>Description</b>	QoS ID.
<b>Parent TLV</b>	R3 QoS Descriptor

2 **5.3.2.228 Media Flow Description in SDP Format**

<b>Type</b>	228
<b>Length in octets</b>	Variable
<b>Value</b>	<SDP string> is encoded as specified in IETF RFC 2327.
<b>Description</b>	This is a variable length string having SDP information. The <SDP string> is encoded as specified in IETF RFC 2327.
<b>Parent TLV</b>	QoS Parameters

3 **5.3.2.229 Capabilities Negotiation Mode**

<b>Type</b>	229
<b>Length in octets</b>	1
<b>Value</b>	Indicates mode being used and is coded as follows: <ul style="list-style-type: none"> <li>• 0x01 = Complete List of Capabilities</li> <li>• 0x02 = Partial List of Capabilities</li> </ul> All other values are Reserved.
<b>Description</b>	Indicates Capability Negotiation Mode to be used
<b>Parent TLV</b>	Capabilities Info

1 **5.3.2.230 R3 Schedule Type**

<b>Type</b>	230
<b>Length</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x02 = Best Effort</li> <li>• 0x03 = nrtPS</li> <li>• 0x04 = rtPS</li> <li>• 0x05 = Extended rtPS</li> <li>• 0x06 = UGS</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Schedule Type.
<b>Parent TLV</b>	R3 QoS Descriptor

2 **5.3.2.231 Certified-for-MBCS**

<b>Type</b>	231
<b>Length</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Certified for MBCS-App</li> <li>• 0x01 = Certified for MBCS-DSx</li> </ul> <p>All other value are Reserved</p>
<b>Description</b>	
<b>Parent TLV</b>	Certified-MS-Feature-List-For-GW

3 **5.3.2.232 Certified-for-LBS**

<b>Type</b>	232
<b>Length</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Certified for LBS Control Plane</li> <li>• 0x01 = Certified for LBS Hybrid</li> </ul> <p>All other value are Reserved</p>
<b>Description</b>	
<b>Parent TLV</b>	Certified-MS-Feature-List-For-GW



1 **5.3.2.233 Certified-for-Compression**

<b>Type</b>	233
<b>Length</b>	1
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"><li>•0x00 = Certified for RoHC</li><li>•0x01 = Certified for PHS</li></ul> All other value are Reserved
<b>Description</b>	
<b>Parent TLV</b>	Certified-MS-Feature-List-For-GW

2 **5.3.2.234 Certified-for-Scan-Capability**

<b>Type</b>	234
<b>Length</b>	1
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"><li>•0x00 = Certified for HO Scanning</li><li>•0x01 = Certified for Scan Report Type Support</li><li>•0x00 = Certified for HO/Scan/Report Trigger Metrics</li></ul> All other value are Reserved
<b>Description</b>	
<b>Parent TLV</b>	Certified-MS-Feature-List-For-BS

3 **5.3.2.235 Certified-for-Security-Capability**

<b>Type</b>	235
<b>Length</b>	1
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"><li>•0x00 = Certified for PKM message encoding support</li><li>•0x01 = Certified for Authorization policy support – Initial Network entry</li><li>•0x02 = Certified for Authorization policy support – Network re-entry</li></ul> All other value are Reserved
<b>Description</b>	
<b>Parent TLV</b>	Certified-MS-Feature-List-For-BS

1 **5.3.2.236 R3 Maximum Latency**

<b>Type</b>	236
<b>Length in octets</b>	4
<b>Value</b>	32-bit integer specifies the maximum latency (in milliseconds).
<b>Description</b>	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.
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>R3 QoS Descriptor</li> </ul>

2 **5.3.2.237 Reduced Resources Code**

<b>Type</b>	237
<b>Length in octets</b>	0
<b>Value</b>	Value = Null, see Description.
<b>Description</b>	This code indicates that the requesting entity will accept reduced resources Code if the requested resources are not available.
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>QoS Parameters</li> <li>R3 QoS Descriptor</li> </ul>

3 **5.3.2.238 R3 Media Flow Type**

<b>Type</b>	238
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>0x01 = Voice over IP</li> <li>0x02 = Robust Browser</li> <li>0x03 = Secure Browser/ VPN</li> <li>0x04 = Streaming video on demand</li> <li>0x05 = Streaming live TV</li> <li>0x06 = Music and Photo Download</li> <li>0x07 = Multi-player gaming</li> <li>0x08 = Location-based services</li> <li>0x09 = Text and Audio Books with Graphics</li> <li>0x0A = Video Conversation</li> <li>0x0B = Message</li> <li>0x0C = Control</li> <li>0x0D = Data</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>R3 QoS Descriptor</li> </ul>

### 5.3.2.239 Certified-for-ARQ-Capability

<b>Type</b>	239
<b>Length</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Certified for Sending and Receiving PDU for ARQ</li> <li>• 0x01 = Certified for ARQ feedback message</li> <li>• 0x02 = Certified for ARQ Discard message</li> <li>• 0x03 = Certified for ARQ Reset message</li> </ul> <p>All other value are Reserved</p>
<b>Description</b>	
<b>Parent TLV</b>	Certified-MS-Feature-List-For-BS

### 5.3.2.240 R3 SDU Size

<b>Type</b>	240
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer. Default = 49.
<b>Description</b>	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).
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>• R3 QoS Descriptor</li> </ul>

### 5.3.2.241 R3 Unsolicited Polling Interval

<b>Type</b>	241
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer representing the polling interval (in milliseconds).
<b>Description</b>	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
<b>Parent TLV</b>	<ul style="list-style-type: none"> <li>• R3 QoS Descriptor</li> </ul>

### 5.3.2.242 R3 Acct Interim Interval

<b>Type</b>	242
<b>Length</b>	4
<b>Value</b>	32-bit unsigned integer
<b>Description</b>	Acct-Interim-Interval.
<b>Parent TLV</b>	Ms Authorization Context

### 5.3.2.243 Accounting Mode Provisioning

In order to support the “optional” accounting agent at the BS to communicate with the Accounting Client, there needs to be messaging over the R6 interface. The following accounting session provisioning TLV is included in existing messages to indicate the different accounting options as described in the Stage 2 specifications.

<b>Type</b>	243		
<b>Length in octets</b>	Variable		
<b>Value</b>	Compound TLV		
<b>Description</b>	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.		
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>Description</b>	<b>M/O</b>
	Accounting Type	The Accounting Type is data field 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 data field in the AAA server and sent to the Accounting Client in the Access_Accept message during Network Entry. This TLV is only used for volume-based accounting. This duration SHALL be kept constant throughout the WiMAX Session of the user.	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 data field 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
<b>Parent TLV(s)</b>	Accounting Context		

### 5.3.2.244 Accounting Session/Flow Volume Counts

<b>Type</b>	244
<b>Length in octets</b>	Variable
<b>Value</b>	Compound TLV

<b>Description</b>	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.		
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>Description</b>	<b>M/O</b>
	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
<b>Parent TLV(s)</b>	Accounting Bulk Session/Flow		

1 **5.3.2.245 Accounting Number of Bulk Sessions/Flows**

<b>Type</b>	245
<b>Length in octets</b>	1
<b>Value</b>	The number of Accounting Bulk Session/Flow TLVs
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Bulk Session/Flow Volume Counts

2 **5.3.2.246 Accounting Bulk Session/Flow**

Type	246		
Length in octets	Variable		
Value	Compound TLV		
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
	Accounting IP Address		M
	SFID		O
	Accounting Session/Flow Volume Counts		M
Parent TLV(s)	Accounting Bulk Session/Flow Volume Counts		

1 **5.3.2.247 Accounting Type**

<b>Type</b>	247
<b>Length in octets</b>	1
<b>Value</b>	1 <sup>st</sup> nibble: <ul style="list-style-type: none"> <li>0x0 = Invalid</li> <li>0x1 = IP Session-Based Accounting Default value for the ASN</li> <li>0x2 = Flow-Based Accounting</li> </ul> All other values are Reserved.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Mode Provisioning

2 **5.3.2.248 Interim Update Interval**

<b>Type</b>	248
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer representing the interval in seconds.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Mode Provisioning

3 **5.3.2.249 Cumulative Uplink Octets**

<b>Type</b>	249
<b>Length in octets</b>	8
<b>Value</b>	Cumulative uplink volume count in octets.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Session/Flow Volume Counts

4 **5.3.2.250 Cumulative Downlink Octets**

<b>Type</b>	250
<b>Length in octets</b>	8
<b>Value</b>	Cumulative downlink volume count in octets.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Session/Flow Volume Counts

5 **5.3.2.251 Cumulative Uplink Packets**

<b>Type</b>	251
<b>Length in octets</b>	8
<b>Value</b>	Cumulative uplink volume count in packets.
<b>Description</b>	

<b>Parent TLV(s)</b>	Accounting Session/Flow Volume Counts
----------------------	---------------------------------------

1 **5.3.2.252 Cumulative Downlink Packets**

<b>Type</b>	252
<b>Length in octets</b>	8
<b>Value</b>	Cumulative downlink volume count in packets.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Session/Flow Volume Counts

2 **5.3.2.253 Time of Day Tariff Switch**

Type	253	
Length in octets	6	
Value	Compound TLV	
Description		
Elements (Sub-TLVs)	TLV Name	M/O
	1. Time of Day Tariff Switch Time	M
	2. Time of Day Tariff Switch Offset	M

3 **5.3.2.254 Time of Day Tariff Switch Time**

<b>Type</b>	254
<b>Length in octets</b>	2
<b>Value</b>	The time of day time in hours and minutes <ul style="list-style-type: none"> <li>Octet 1: 0x00-0x17 = Hour (0-23)</li> <li>Octet 2: 0x00-0x3B = Minute (0-59)</li> </ul> All other values are Reserved.
<b>Description</b>	
<b>Parent TLV(s)</b>	Time of Day Tariff Switch

4 **5.3.2.255 Time of Day Tariff Switch Offset**

<b>Type</b>	255
<b>Length in octets</b>	4
<b>Value</b>	32-bit signed integer: Offset (+/- seconds from UTC).
<b>Description</b>	
<b>Parent TLV(s)</b>	Time of Day Tariff Switch

5 **5.3.2.256 Accounting Number of ToDs**

<b>Type</b>	256
<b>Length in octets</b>	1

<b>Value</b>	UINT8 (0 .. 255).
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Mode Provisioning

1 **5.3.2.257 Uplink Octets at Tariff Switch**

<b>Type</b>	257
<b>Length in octets</b>	8
<b>Value</b>	Uplink octets at tariff switch.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Session/Flow Volume Counts

2 **5.3.2.258 Downlink Octets at Tariff Switch**

<b>Type</b>	258
<b>Length in octets</b>	8
<b>Value</b>	Downlink Octets at Tariff Switch.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Session/Flow Volume Counts

3 **5.3.2.259 Uplink Packets at Tariff Switch**

<b>Type</b>	259
<b>Length in octets</b>	8
<b>Value</b>	Uplink Packets at tariff switch.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Session/Flow Volume Counts

4 **5.3.2.260 Downlink Packets at Tariff Switch**

<b>Type</b>	260
<b>Length in octets</b>	8
<b>Value</b>	Downlink Packets at tariff switch.
<b>Description</b>	
<b>Parent TLV(s)</b>	Accounting Session/Flow Volume Counts

5 **5.3.2.261 Vendor Specific TLV**

6 Vendor Specific TLV is an optional TLV. When TLV type indicates Vendor Specific TLV, but the Vendor ID is  
7 not recognized, then processing SHALL silently discard the TLV and continue processing the rest of the message.

8 The value field of the TLV contains the Vendor Identification (Vendor ID) specified by the 24-bit vendor-specific  
9 Organization Unique Identifier (OUI) of the Network Element Vendor or Network Provider.



1 The content and format of the TLV is as follows:

<b>Type</b>	0x7FFF (524287)
<b>Length in Octets</b>	Variable
<b>Value</b>	Vendor Specific information Field (VSIF).
<b>Description</b>	
<b>Message Primitives That Use This TLV</b>	Every message

2 The format of the Vendor Specific Information Field (VSIF) is as follows:

- 3 • First 24 bits – Vendor ID (mandatory)
- 4 • Rest of info in TLV (optional) – vendor-specific, out of scope for standard definition

5 The Vendor ID field SHALL be the first field of VSIF.

6 Vendor Specific TLV MAY be nested inside another TLV.

7 Multiple Vendor Specific TLVs can be inserted into one message across R6 or R4.

## 8 Notes

9 Note 1: Vendor ID mentioned in this section is different from the Vendor ID specified in Section 4 and Section  
10 5.4.2. Vendor ID in this section refers only to Organization Unique Identifier (OUI) of the Network Element Vendor  
11 or Network Provider and does not refer to Enterprise Number.

12 Note 2: One or more SF Info TLVs MAY be included in order to describe Service Flows in Data Path Control,  
13 Reservation, and HO Control Messages. In Data Path Control SF Info is included for Per-SF data path tunneling  
14 granularity.

15 Note 3: For Per-SF data path tunneling granularity, DP Info SHALL be included as sub-TLV of SF Info

16 Note 4: Anchor ASN GW ID points to the network entity that hosts Anchor DPF or anchor ASN GW. The content  
17 is IP address (v4 or v6).

18 It does not have to be included if AK Context is included. If neither Authenticator ID nor AK Context is  
19 included means that the sender of the *HO\_Req* hosts the Authenticator Function for the MS.

20 Anchor ASN GW ID points to the network entity that hosts Anchor DPF or anchor ASN GW. The content  
21 is IP address (v4 or v6).

## 22 5.3.2.262Paging Preference

<b>Type</b>	262
<b>Length in octets</b>	1
<b>Value</b>	Refer to 802.16e section 11.13.30.
<b>Description</b>	This parameter is a single bit indicator of an MS's preference for the reception of paging advisory messages during idle mode. When set, it indicates that the BS may present paging advisory messages or other indicative messages to the MS when data SDUs bound for the MS are present while the MS is in idle mode.
<b>Parent TLV</b>	SF Info

1 **5.3.2.263 Void**

2 **5.3.2.264 Accounting IP Address**

<b>Type</b>	264
<b>Length in octets</b>	Variable (either 4 or 16)
<b>Value</b>	
<b>Description</b>	
<b>Parent TLV</b>	Accounting Bulk Session/Flow

3 **5.3.2.265 Data Delivery Trigger**

<b>Type</b>	265
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = No trigger</li> <li>• 0x01 = Triggers immediate delivery of data for the specified Service Flow</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Triggers data delivery for the specified service flow.
<b>Parent TLV</b>	SF Info

4 **5.3.2.266 MIP4 Security Info**

<b>Type</b>	266	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	MIP4 security context to be transferred from Anchor Authenticator to FA.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	MN-FA Key	O
	MN-FA Key Lifetime	O
	MN-FA SPI	O
	MS NAI	O
	PMIP-Authenticated-Network-Identity	O
	FA-HA Key	O
	FA-HA Key Lifetime	O
	FA-HA SPI	O
	HA IP Address	O
<b>Message Primitive(s) that use this TLV</b>	Context_Rpt	

1 **5.3.2.267 MN-FA Key Lifetime**

<b>Type</b>	267
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Time of MN-FA key remaining valid. This is provided to the FA by the anchor Authenticator for MN-FA key context transfer.
<b>Parent TLV(s)</b>	MIP4 Security Info

2 **5.3.2.268 Idle Mode Timeout**

<b>Type</b>	268
<b>Length in octets</b>	2 (as specified in 802.16e)
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	Maximum time interval between MS idle mode location updates in seconds, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	Paging Information, REG Context

3 **5.3.2.269 Classification Result**

<b>Type</b>	269
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>0x00 = None</li> <li>0x01 = Discard packet</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	The value of this field specifies an action associated with the classification rule. If it is present in the Packet Classification Rule, its action SHALL be applied on the packets that match this classification rule.
<b>Parent TLV(s)</b>	Packet Classification Rule / Media Flow Description

4 **5.3.2.270 Network assisted HO Supported**

<b>Type</b>	270
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>0x00 = Network Assisted HO not supported</li> <li>0x01 = Network Assisted HO supported</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Defined in [11] Indicator for network assisted HO.
<b>Message Primitives That Use This TLV</b>	HO_Directive

1 **5.3.2.271 Destination Identifier**

<b>Type</b>	271
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets).
<b>Value</b>	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.
<b>Description</b>	Unique identifier for the message destination.
<b>Parent TLV</b>	None

2 **5.3.2.272 Source Identifier**

<b>Type</b>	272
<b>Length in octets</b>	Variable (could be of three fixed sized: 4, 6 and 16 octets).
<b>Value</b>	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.
<b>Description</b>	Unique identifier for the message source.
<b>Parent TLV</b>	None

3 **5.3.2.273 R3 Relocation Action**

<b>Type</b>	273
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = None</li> <li>• 0x01 = Initiate Paging</li> <li>• 0x02 = Initiate FA Migration</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	R3 Relocation Action Code.
<b>Message Primitives That use this TLV</b>	Relocation_Ready_Rsp

1 **5.3.2.274 Ungraceful Network Exit Indicator**

<b>Type</b>	274
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 – Ungraceful Network Exit No Reason</li> <li>• 0x01 – AAA initiated Ungraceful Network Exit</li> <li>• 0x02 – Authenticator initiated Ungraceful Network Exit</li> <li>• 0x03 – Ungraceful Network Exit by MIP session termination</li> <li>• 0x04 – PC initiated Ungraceful Network Exit</li> </ul> <p>All other values are Reserved. If a Reserved value is received then it SHALL be treated by Receiver as if received value 0x00.</p>
<b>Description</b>	This TLV indicates the cause of the ungraceful Network Exit. This TLV SHALL be included to indicate an ungraceful network exit. The default value is 0x00 for the transmitter and the interpretation of the values is optional for the receiver.
<b>Message Primitives That Use This TLV</b>	NetExit_MS_State_Change_Req

2 **5.3.2.275 Duration Quota**

<b>Type</b>	275
<b>Length in octets</b>	4
<b>Value</b>	Unsigned Integer representing seconds.
<b>Description</b>	This optional TLV is only present if duration-based charging is used. It indicates the duration (in seconds) allocated for the session. It is encoded as an integer. It may indicate the total duration (in seconds) since the start of the accounting session related to the QuotaID of the PPAQ in which it occurs.
<b>Parent TLV(s)</b>	PPAQ

3 **5.3.2.276 Duration Threshold**

<b>Type</b>	276
<b>Length in octets</b>	4
<b>Value</b>	Unsigned Integer representing seconds.
<b>Description</b>	This TLV is optionally present if DurationQuota is present. It 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.
<b>Parent TLV(s)</b>	PPAQ

1 **5.3.2.277 Resource Quota**

<b>Type</b>	277
<b>Length in octets</b>	4
<b>Value</b>	Unsigned Integer representing a resource measured in units.
<b>Description</b>	This optional TLV is only present if resource-based or one-time charging is used. It indicates the resources allocated for the session. It may indicate 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.
<b>Parent TLV</b>	PPAQ

2 **5.3.2.278 Resource Threshold**

<b>Type</b>	278
<b>Length in octets</b>	4
<b>Value</b>	Unsigned Integer representing a resource measured in units.
<b>Description</b>	The semantics of this TLV follows those of the Volume Threshold and DurationThreshold.
<b>Parent TLV</b>	PPAQ

3 **5.3.2.279 Update Reason**

<b>Type</b>	279
<b>Length in octets</b>	1
<b>Value</b>	<ul style="list-style-type: none"> <li>• Enumerator. The values are: 0x01 = Pre-initialization</li> <li>• 0x02 = Initial-Request</li> <li>• 0x03 = Threshold Reached</li> <li>• 0x04 = Quota Reached</li> <li>• 0x05 = TITSU Approaching</li> <li>• 0x06 = Remote Forced Disconnect</li> <li>• 0x07 = Client Service Termination</li> <li>• 0x08 = “Access Service” Terminated</li> <li>• 0x09 = Service not established</li> <li>• 0x0A = One-time Charging</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	This TLV SHALL be present in the quota update messages. 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.
<b>Parent TLV</b>	PPAQ

### 5.3.2.280 Service-ID

<b>Type</b>	280
<b>Length in octets</b>	Variable
<b>Value</b>	The value field of this TLV is encoded as a string.
<b>Description</b>	<p>This value is handled as an opaque string that uniquely describes the service instance to which prepaid metering should be applied. In the Context of Hot-Lining; it identifies the Hotlining Context on the Expiry of PPAQ with Same Service ID.</p> <p>The Service-Id is represented as an IP 5-tuple (source address, source port, destination address, destination port, protocol).</p> <p>If a Service-ID 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).</p>
<b>Parent TLV</b>	PPAQ, Hotlining Context

### 5.3.2.281 Rating-Group-ID

<b>Type</b>	281
<b>Length in octets</b>	4
<b>Value</b>	Unsigned Integer representing the value of the Rating Group ID.
<b>Description</b>	This TLV 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.
<b>Parent TLV</b>	PPAQ

### 5.3.2.282 Termination Action

<b>Type</b>	282
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>0x00x01 = Terminate</li> <li>0x02 = Request more quota</li> <li>0x03 = Redirect/Filter</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	This TLV describes action to take when the PPS does not grant additional quota.
<b>Parent TLV</b>	PPAQ

### 5.3.2.283 Pool-ID

<b>Type</b>	283
<b>Length in octets</b>	4
<b>Value</b>	Unsigned Integer representing a Pool-ID.
<b>Description</b>	This TLV identifies the resource pool that the quota included in this PPAQ is associated with.
<b>Parent TLV</b>	PPAQ

### 5.3.2.284 Pool-Multiplier

<b>Type</b>	284
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	The pool-multiplier determines the weight that resources are inserted into the pool that is identified by the accompanying Pool-ID, and the rate at which resources are taken out of the pool by the relevant Service or Rating-Group.
<b>Parent TLV</b>	PPAQ

### 5.3.2.285 Prepaid Server

<b>Type</b>	285
<b>Length in octets</b>	4 (IPv4) or 16 (IPv6)
<b>Value</b>	The attribute consists of an unsigned integer.
<b>Description</b>	Indicates the address (IPv4 or IPv6) of the serving PPS. Multiple instances of this subtype MAY be present in a single PPAQ. If provided by HAAA, PPC must include it in the subsequent R3 messages. It is a part of PPC context.
<b>Parent TLV</b>	PPAQ

### 5.3.2.286 R3 Active Time

<b>Type</b>	286
<b>Length</b>	4
<b>Value</b>	32-bit unsigned Integer.
<b>Description</b>	The number of seconds the session was not in Idle Mode.
<b>Parent TLV</b>	Accounting Context



### 5.3.2.287 Interim Update Interval Remaining

<b>Type</b>	287
<b>Length</b>	4
<b>Value</b>	32-bit unsigned Integer.
<b>Description</b>	The number of seconds remaining in the current Interim Update Interval.
<b>Parent TLV</b>	Accounting Context

### 5.3.2.288 Number of UL Transport CIDs Support

<b>Type</b>	288
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	The number of uplink Transport CIDs supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

### 5.3.2.289 Number of DL Transport CIDs Support

<b>Type</b>	289
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	The number of downlink Transport CIDs supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

### 5.3.2.290 Classification/PHS Options and SDU Encapsulation Support

<b>Type</b>	290
<b>Length in octets</b>	2 or 4
<b>Value</b>	16 or 32-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This TLV contains information of Classification/PHS options and SDU encapsulation which are supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

### 5.3.2.291 Maximum Number of Classifier

<b>Type</b>	291
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	Maximum number of simultaneously admitted classification rules supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

1 **5.3.2.292 PHS Support**

<b>Type</b>	292
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	This TLV indicates which type of PHS is supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

2 **5.3.2.293 ARQ Support**

<b>Type</b>	293
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	This TLV indicates if ARQ is supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

3 **5.3.2.294 DSx Flow Control**

<b>Type</b>	294
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	This TLV indicates how many concurrent transactions of DSx messages are supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

4 **5.3.2.295 Total Number of Provisioned Service Flows**

<b>Type</b>	295
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Total number of pre-provisioned service flows supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

1 **5.3.2.296 Maximum MAC Data per Frame Support**

<b>Type</b>	296	
<b>Length</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>	Maximum amount of MAC data per air frame supported by BS and MS, as defined in IEEE802.16e.	
<b>Elements</b>	<b>TLV Name</b>	<b>M/O</b>
	Maximum amount of MAC Level Data per DL Frame	M
	Maximum amount of MAC Level Data per UL Frame	M
<b>Parent TLV</b>	REG Context	

2 **5.3.2.297 Maximum amount of MAC Level Data per DL Frame**

<b>Type</b>	297
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer. A value of 0x0000 means unlimited.
<b>Description</b>	Maximum amount of downlink MAC data per air frame supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	Maximum MAC Data per Frame Support

3 **5.3.2.298 Maximum amount of MAC Level Data per UL Frame**

<b>Type</b>	298
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer. A value of 0x0000 means unlimited.
<b>Description</b>	Maximum amount of uplink MAC data per air frame supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	Maximum MAC Data per Frame Support

4 **5.3.2.299 Packing Support**

<b>Type</b>	299
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	This TLV indicates if packing of fragments is supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

1 **5.3.2.300 MAC ertPS Support**

<b>Type</b>	300
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	This TLV indicates if ertPS scheduling type in the MAC layer is supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

2 **5.3.2.301 Maximum Number of Bursts Transmitted Concurrently to the MS**

<b>Type</b>	301
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Maximum number of bursts transmitted concurrently to the MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

3 **5.3.2.302 HO Supported**

<b>Type</b>	302
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This TLV indicates which type of handovers is supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

4 **5.3.2.303 HO Process Optimization MS Timer**

<b>Type</b>	303
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	The duration in frames the MS SHALL wait until receipt of the next unsolicited network reentry MAC management message, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

5 **5.3.2.304 Mobility Features Supported**

<b>Type</b>	304
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This TLV indicates if handover, sleep mode, and idle mode are supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context, RRM BS Info

1 **5.3.2.305 Sleep Mode Recovery Time**

<b>Type</b>	305
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Number of frames required for the MS to switch from sleep mode to awake mode, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

2 **5.3.2.306 Void**

3 **5.3.2.307 ARQ Ack Type**

<b>Type</b>	307
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This TLV indicates which types of ARQ Ack types are supported by BS and MS, as defined in IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

4 **5.3.2.308 MS HO Connections Parameters Proc Time**

<b>Type</b>	308
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Time in ms the MS needs to process information on connections during HO, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

5 **5.3.2.309 MS HO TEK Proc Time**

<b>Type</b>	309
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Time in ms the MS needs to process TEK information during HO, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

1 **5.3.2.310 MAC Header and Extended Sub-Header Support**

<b>Type</b>	310
<b>Length in octets</b>	3
<b>Value</b>	24-bit bitmask, as specified in IEEE802.16e.
<b>Description</b>	This TLV indicates which types of MAC headers and sub-headers are supported by BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

2 **5.3.2.311 System Resource Retain Timer**

<b>Type</b>	311
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	System resource retain timer set by the BS during the initial network entry of MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

3 **5.3.2.312 MS Handover Retransmission Timer**

<b>Type</b>	312
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	MS Handover Retransmission Timer set by the BS during the initial network entry of MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

4 **5.3.2.313 Handover Indication Readiness Timer**

<b>Type</b>	313
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	MS Handover Indication Readiness Timer agreed by the BS and MS during the initial network entry of MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

5 **5.3.2.314 BS Switching Timer**

<b>Type</b>	314
<b>Length in octets</b>	1
<b>Value</b>	8-bit coded value, as specified in the IEEE802.16e.
<b>Description</b>	Minimum time from transmission of MOB_HO-IND at the serving BS until proper reception of Fast_Rangin IE at the target BS, as specified in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

1 **5.3.2.315 Power Saving Class Capability**

<b>Type</b>	315
<b>Length in octets</b>	2
<b>Value</b>	16-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This TLV indicates which types of power saving classes are supported by BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	REG Context

2 **5.3.2.316 Subscriber Transition Gaps**

<b>Type</b>	316
<b>Length in octets</b>	2
<b>Value</b>	16-bit coded value, as specified in the IEEE802.16e.
<b>Description</b>	This TLV indicates the transition gap SSTTG and SSRTG for TDD and H-FDD SSs, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

3 **5.3.2.317 Maximum Transmit Power**

<b>Type</b>	317
<b>Length in octets</b>	4
<b>Value</b>	32-bit coded value, as specified in the IEEE802.16e.
<b>Description</b>	The maximum available power for BPSK, QPSK, 16-QAM, and 64-QAM constellations, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

4 **5.3.2.318 Capabilities for Construction and Transmission of MAC PDUs**

<b>Type</b>	318
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	Indicates the capabilities for construction and transmission of MAC PDUs.
<b>Parent TLV(s)</b>	SBC Context

5 **5.3.2.319 PKM Flow Control**

<b>Type</b>	319
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Maximum number of concurrent PKM transactions supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

1 **5.3.2.320 Maximum Number of Supported Security Associations**

<b>Type</b>	320
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Maximum number of security association supported by the SS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

2 **5.3.2.321 Security Negotiation Parameters**

<b>Type</b>	321	
<b>Length</b>	Variable	
<b>Value</b>	Compound TLV	
<b>Description</b>	Security parameters that has been agreed between MS and BS and delivered in SBC-RSP message during the initial network entry of MS.	
<b>Elements</b>	<b>TLV Name</b>	<b>M/O</b>
	Authorization Policy Support	M
	MAC Mode	M
	PN Window Size	M
<b>Parent TLV</b>	SBC Context	

3 **5.3.2.322 Void**

4 **5.3.2.323 MAC Mode**

<b>Type</b>	323
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates which message authentication code mode is supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	Security Negotiation Parameters

5 **5.3.2.324 PN Window Size**

<b>Type</b>	324
<b>Length in octets</b>	2
<b>Value</b>	16-bit unsigned integer.
<b>Description</b>	Size of the receiver PN window for SAs and management connections supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	Security Negotiation Parameters

6 **5.3.2.325 Extended Subheader Capability**

<b>Type</b>	325
-------------	-----



<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	Extended subheader capability supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

1 **5.3.2.326HO Trigger Metric Support**

<b>Type</b>	326
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates which trigger metrics are supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

2 **5.3.2.327Current Transmit Power**

<b>Type</b>	327
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	This indicates the transmitted power used for the burst which carried the SBC-REQ message, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

3 **5.3.2.328OFDMA SS FFT Sizes**

<b>Type</b>	328
<b>Length in octets</b>	1
<b>Value</b>	This indicates FFT size supported by the BS and MS, as defined in the IEEE802.16e.
<b>Description</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

4 **5.3.2.329OFDMA SS demodulator**

<b>Type</b>	329
<b>Length in octets</b>	variable
<b>Value</b>	Sets of 16-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates MS demodulator options supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

5 **5.3.2.330OFDMA SS modulator**

<b>Type</b>	330
-------------	-----

<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates MS modulator options supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

1 **5.3.2.331 The number of UL HARQ Channel**

<b>Type</b>	331
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	The number of UL_HARQ channels supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

2 **5.3.2.332 OFDMA SS Permutation support**

<b>Type</b>	332
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	This indicates which OFDMA permutation modes are supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

3 **5.3.2.333 OFDMA SS CINR Measurement Capability**

<b>Type</b>	333
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates which channel quality measurement methods are supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

4 **5.3.2.334 The number of DL HARQ Channels**

<b>Type</b>	334
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	The number of DL_HARQ channels supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

5 **5.3.2.335 HARQ Chase Combining and CC-IR Buffer Capability**

<b>Type</b>	335
-------------	-----

<b>Length in octets</b>	2
<b>Value</b>	16-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates if HARQ Chase Combining and CC-IR buffer are supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

1 **5.3.2.336 OFDMA SS Uplink Power Control Support**

<b>Type</b>	336
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates which power control methods for uplink are supported by MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

2 **5.3.2.337 OFDMA SS Uplink Power Control Scheme Switching Delay**

<b>Type</b>	337
<b>Length in octets</b>	1
<b>Value</b>	8-bit unsigned integer.
<b>Description</b>	Minimum number of frames that MS takes to switch between open-loop and closed-loop power control schemes, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

3 **5.3.2.338 OFDMA MAP Capability**

<b>Type</b>	338
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates which MAP options are supported by the BS and MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

4 **5.3.2.339 Uplink Control Channel Support**

<b>Type</b>	339
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates which uplink control channels are supported by MS, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

5 **5.3.2.340 OFDMA MS CSIT Capability**

<b>Type</b>	340
-------------	-----

<b>Length in octets</b>	2
<b>Value</b>	16-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	This indicates MS capability of supporting CSIT (UL sounding), as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

1 **5.3.2.341 Maximum Number of Burst per Frame Capability in HARQ**

<b>Type</b>	341
<b>Length in octets</b>	1
<b>Value</b>	8-bit coded value, as specified in the IEEE802.16e.
<b>Description</b>	This indicates the maximum number of UL/DL data burst allocations for the SS in a single UL/DL subframe, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

2 **5.3.2.342 OFDMA SS demodulator for MIMO Support**

<b>Type</b>	342
<b>Length in octets</b>	3
<b>Value</b>	24-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	MIMO capability of MS demodulator, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

3 **5.3.2.343 OFDMA SS modulator for MIMO Support**

<b>Type</b>	343
<b>Length in octets</b>	2
<b>Value</b>	16-bit bitmask, as specified in the IEEE802.16e.
<b>Description</b>	MIMO capability of MS modulator, as defined in the IEEE802.16e.
<b>Parent TLV(s)</b>	SBC Context

### 1 5.3.2.344 ARQ Context

<b>Type</b>	344	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Contains ARQ related information of the service flow.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	ARQ WINDOW SIZE	O
	ARQ RETRY TIMEOUT-Transmitter Delay	O
	ARQ RETRY TIMEOUT-Receiver Delay	O
	ARQ BLOCK LIFETIME	O
	ARQ SYNC LOSS TIMEOUT	O
	ARQ DELIVER IN ORDER	O
	ARQ RX PURGE TIMEOUT	O
	ARQ BLOCK SIZE	O
	RECEIVER ARQ ACK PROCESSING TIME	O
<b>Parent TLV(s)</b>	SF Info	

2

### 3 5.3.2.345 ARQ Enable

<b>Type</b>	345	
<b>Length in octets</b>	1	
<b>Value</b>	Enumerator. The values are: <ul style="list-style-type: none"> <li>• 0x00 = ARQ Not Requested/Accepted</li> <li>• 0x01 = ARQ Requested/Accepted</li> </ul> All other values are Reserved.	
<b>Description</b>	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.	
<b>Parent TLV</b>	SF Info	

### 4 5.3.2.346 ARQ WINDOW SIZE

<b>Type</b>	346	
<b>Length in octets</b>	2	
<b>Value</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.	
<b>Description</b>	This parameter is negotiated upon connection setup or during operation as defined in IEEE802.16e.	
<b>Parent TLV</b>	ARQ Context	

### 5 5.3.2.347 ARQ RETRY TIMEOUT-Transmitter Delay

<b>Type</b>	347	
-------------	-----	--

<b>Length in octets</b>	2
<b>Value</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
<b>Description</b>	This is the total transmitter delay, including sending and receiving delays and other implementation dependent processing delays as defined in IEEE802.16e.
<b>Parent TLV</b>	ARQ Context

1 **5.3.2.348 ARQ RETRY TIMEOUT-Receiver Delay**

<b>Type</b>	348
<b>Length in octets</b>	2
<b>Value</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
<b>Description</b>	This is the total receiver delay, including receiving and sending delays and other implementation-dependent processing delays as defined in IEEE802.16e.
<b>Parent TLV</b>	ARQ Context

2 **5.3.2.349 ARQ BLOCK LIFETIME**

<b>Type</b>	349
<b>Length in octets</b>	2
<b>Value</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
<b>Description</b>	Indicates the lifetime of ARQ block as defined in IEEE802.16e.
<b>Parent TLV</b>	ARQ Context

3 **5.3.2.350 ARQ SYNC LOSS TIMEOUT**

<b>Type</b>	350
<b>Length in octets</b>	2
<b>Value</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
<b>Description</b>	Indicates the maximum time interval after which loss of synchronization is indicated as defined in IEEE802.16e.
<b>Parent TLV</b>	ARQ Context

4 **5.3.2.351 ARQ DELIVER IN ORDER**

<b>Type</b>	351
<b>Length in octets</b>	1
<b>Value</b>	As defined in IEEE802.16e.
<b>Description</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
<b>Parent TLV</b>	ARQ Context

5 **5.3.2.352 ARQ RX PURGE TIMEOUT**

<b>Type</b>	352
<b>Length in octets</b>	2

<b>Value</b>	As defined in IEEE802.16e.
<b>Description</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
<b>Parent TLV</b>	ARQ Context

1 **5.3.2.353 ARQ BLOCK SIZE**

<b>Type</b>	353
<b>Length in octets</b>	2
<b>Value</b>	As defined in IEEE802.16e.
<b>Description</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
<b>Parent TLV</b>	ARQ Context

2 **5.3.2.354 RECEIVER ARQ ACK PROCESSING TIME**

<b>Type</b>	354
<b>Length in octets</b>	1
<b>Value</b>	As defined in IEEE802.16e.
<b>Description</b>	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
<b>Parent TLV</b>	ARQ Context

3 **5.3.2.355 State**

<b>Type</b>	355
<b>Length in octets</b>	Variable 1-253 octets
<b>Value</b>	Octet String
<b>Description</b>	State attribute as received in most recent message from AAA server.
<b>Parent TLV(s)</b>	MS Info

4

5 **5.3.2.356 R3 Media Flow Description in SDP Format**

<b>Type</b>	356
<b>Length in octets</b>	Variable
<b>Value</b>	<SDP string> is encoded as specified in IETF RFC 2327.
<b>Description</b>	This is a variable length string having SDP information. The <SDP string> is encoded as specified in IETF RFC 2327.
<b>Parent TLV</b>	R3 QoS descriptor

6 **5.3.2.357 VolumeUsed**

<b>Type</b>	357
<b>Length in octets</b>	4
<b>Value</b>	The attribute is an unsigned Integer representing a volume measured in kilo-bytes (1024 bytes).

<b>Description</b>	This TLV describes the total used volume (in octets) for both inbound and outbound traffic.
<b>Parent TLV(s)</b>	PPAQ

1 **5.3.2.358 Time Stamp**

<b>Type</b>	358
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Time stamp for the message transmission time. Time Stamp will be in 24 hour format with granularity in milliseconds since January 1, 1970 00:00 UTC. The 5 most significant bits are set to zero.
<b>Parent TLV(s)</b>	BS Info

2 **5.3.2.359 Accounting Bulk Session/Flow Volume Counts**

Type	359		
Length in octets	Variable		
Value			
Description	The volume count information for several sessions or service flows.		
Elements (Sub-TLVs)	TLV Name	Description	M/O
	Accounting Number of Bulk Sessions/Flows		M
	Accounting Bulk Session/Flow		M
Parent TLV(s)	Offline Accounting Context		

3 **5.3.2.360 Offline Accounting Context**

Type	360	
Length in octets	Variable	
Value	Compound	
Description	Accounting context for Offline accounting	
Elements (Sub-TLVs)	TLV Name	M/O
	Accounting Bulk Session/Flow Volume Counts	M
Message Primitives That Use This TLV	RR_Rsp, Bulk Interim Update, Path_Dereg_Req, IM_Entry_State_Change_Req, NetExit_MS_State_Change_Req, NetExit_MS_State_Change_Rsp, Context_Rpt	

4 **5.3.2.361 R3 Acct Session Time**

<b>Type</b>	361
<b>Length</b>	4



<b>Value</b>	32-bit unsigned Integer
<b>Description</b>	The number of seconds the flow or session was active.
<b>Parent TLV</b>	Accounting Context

1 **5.3.2.362 R3 Visited-Framed-IP-Address**

<b>Type</b>	362
<b>Length</b>	4
<b>Value</b>	32-bit unsigned integer
<b>Description</b>	R3 Visited Framed-IP-Address.
<b>Parent TLV</b>	MS Authorization Context

2 **5.3.2.363 R3 Visited-Framed-IPv6-Prefix**

<b>Type</b>	363
<b>Length</b>	Variable
<b>Value</b>	0-128 bits
<b>Description</b>	R3 Visited Framed-IPv6-Prefix.
<b>Parent TLV</b>	MS Authorization Context

3 **5.3.2.364 R3 Framed-Interface-Id**

<b>Type</b>	364
<b>Length</b>	Variable
<b>Value</b>	8 bytes
<b>Description</b>	R3 Framed-Interface-Id.
<b>Parent TLV</b>	MS Authorization Context

4 **5.3.2.365 R3 Visited-Framed-Interface-Id**

<b>Type</b>	365
<b>Length</b>	Variable
<b>Value</b>	8 bytes
<b>Description</b>	R3 Visited-Framed-Interface-Id.
<b>Parent TLV</b>	MS Authorization Context

5 **5.3.2.366 Delete MS Context Indication**

<b>Type</b>	366
<b>Length</b>	1
<b>Value</b>	Unsigned Integer
<b>Description</b>	Indicates the release of the MS context.
<b>Parent TLV</b>	None

1 **5.3.2.367HO Authorization Policy Support**

<b>Type</b>	367
<b>Length in octets</b>	1
<b>Value</b>	8-bit bitmask with the following values: <ul style="list-style-type: none"> <li>• Bit #0 = RSA authorization</li> <li>• Bit #1 = EAP authorization</li> <li>• Bit #3 = HMAC supported</li> <li>• Bit #4 = CMAC supported</li> <li>• Bit #5 = 64-bit Short-HMAC</li> <li>• Bit #6 = 80-bit Short-HMAC</li> <li>• Bit #7 = 96-bit Short-HMAC</li> </ul> All other bits are Reserved.
<b>Description</b>	This parameter is used to indicate that the authorization policy for the target BS is negotiated. Refer HO Authorization policy support in 802.16e(Cor2/D3).
<b>Parent TLV</b>	BS Info

2 **5.3.2.368NSP ID**

<b>Type</b>	368
<b>Length in octets</b>	3
<b>Value</b>	24-bits NSP ID
<b>Description</b>	Identifier of the NSP.
<b>Parent TLV</b>	MS Info

3 **5.3.2.369Idle Mode Exit Indicator**

<b>Type</b>	369
<b>Length in octets</b>	1
<b>Value</b>	Enumerated. The values are: <ul style="list-style-type: none"> <li>• 0x00 = Idle Mode Exit</li> <li>• 0x01 = MS in Idle Mode</li> </ul> All other values are Reserved.
<b>Description</b>	Present in operations related to MS Idle Mode Exit and indicates whether MS's Serving ASN has MS Context.
<b>Message Primitives that use this TLV</b>	CMAC_Key_Count_Update, IM_Exit_State_Ind

4 **5.3.2.370Failure Indication Details**

<b>Type</b>	370
<b>Length in octets</b>	Variable
<b>Value</b>	Compound

<b>Description</b>	Contains details in addition to the information provided by the Failure Indication TLV. <ul style="list-style-type: none"> <li>If the WiMAX message TLV position TLV is present, it SHALL indicate the occurrence of a TLV in which an error was diagnosed by the message receiver.</li> </ul>	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	WiMAX message TLV position	O (Note 1)
<b>Parent TLV(s)</b>	None.	
<b>Message Primitives that use this TLV</b>	Any error message (Error Response message or Error Reflection message, see 3.4.2).	

1 Note 1: If this TLV is missing, the receiver SHALL ignore the Failure Indication Details TLV.

### 2 5.3.2.371 WiMAX message TLV position

<b>Type</b>	371
<b>Length in octets</b>	$3 * n \ (n \geq 1)$
<b>Value</b>	A sequence of n times <ul style="list-style-type: none"> <li>2 bytes indicating a TLV Type (see section 5.3.1), to be called <math>T_k</math> below</li> <li>an 8-bit unsigned integer, to be called <math>R_k</math> below</li> </ul> where $k = 0, \dots, n - 1$ .
<b>Description</b>	This TLV identifies an occurrence of a TLV, the "reported TLV", in a received message: $TLV_0$ is the reported TLV; $TLV_k$ is the parent TLV of $TLV_{k-1}$ ( $k = 1, \dots, n-1$ ); $TLV_{n-1}$ is a top-level TLV; $T_k$ is the Type of $TLV_k$ ( $k = 0, \dots, n-1$ ); $R_k$ is the repetition number of $TLV_k$ at the message level ( $k = n-1$ ) or at the level of $TLV_{k+1}$ ( $0 \leq k < n-1$ )
<b>Parent TLV</b>	Failure Indication Details

### 3 5.3.2.372 FA Security Info

Type	372	
Length in octets	Variable	
Value	Compound	
Description	Information about the MIP4 Security Info for FA	
Elements (Sub-TLVs)	TLV Name	M/O
	MN-FA Key	O
	MN-FA Key Lifetime	O
	MN-FA SPI	O
	FA-HA Key	O
	FA-HA SPI	O

	FA-HA Key Lifetime	O
<b>Message Primitives That Use This TLV</b>	Context_Rpt	

1 **5.3.2.373 PMIP4 Context**

<b>Type</b>	373	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	MIP4 Information about the MS.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	MIP4 Info	M
<b>Message Primitives That Use This TLV</b>	Relocation_Complete_Rsp	

2 **5.3.2.374 DNS IP Address**

<b>Type</b>	374	
<b>Length in octets</b>	Variable (either 4 or 16 bytes)	
<b>Value</b>	IPv4 or IPv6 address.	
<b>Description</b>	DNS server IP address	
<b>Parent TLV(s)</b>	DHCP Proxy Info	

3

4 **5.3.2.375 Refresh IP Address Trigger**

<b>Type</b>	375	
<b>Length in octets</b>	1	
<b>Value</b>	<p>0 = Triggers BS to set the HO Process Optimization TLV settings in order for MS to perform "Full network entry without traffic IP address refresh (no optimization)" in RNG-RSP.</p> <p>1 = Triggers BS to set the HO Process Optimization TLV settings in order for MS to perform "Traffic IP address refresh (with optimization) without full network entry" in RNG-RSP.</p>	
<b>Description</b>	Triggers BS to prompt MS for refreshing its IP address.	
<b>Message Primitives That Use This TLV</b>	<p>IM_Exit_State_Change_Rsp</p> <p>A WiMAX Release prior to 1.5 will not understand the meaning of this TLV.</p>	

5

### 5.3.2.376 Authorized Network Services

<b>Type</b>	376
<b>Length in octets</b>	4
<b>Value</b>	<p>4 octet Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• 0x00000001 – CMIP4</li> <li>• 0x00000002 – PMIP4</li> <li>• 0x00000004 – Simple IPv4</li> <li>• 0x00000008 – CMIP6</li> <li>• 0x00000010 – PMIP6</li> <li>• 0x00000020 – Simple IPv6</li> <li>• 0x00000040 – Simple ETH Service</li> <li>• 0x00000080 – MIP based ETH Service</li> <li>• 0x00000100 = L2 DHCP Relay<sup>[a]</sup></li> <li>• The rest of the bits are reserved</li> </ul>
<b>Description</b>	This TLV indicates the network service capabilities ASN is authorized to support
<b>Parent TLV</b>	MS Authorization Context

[a] L2 DHCP Relay MAY be selected with either Simple Ethernet Service or MIP based Ethernet Service.

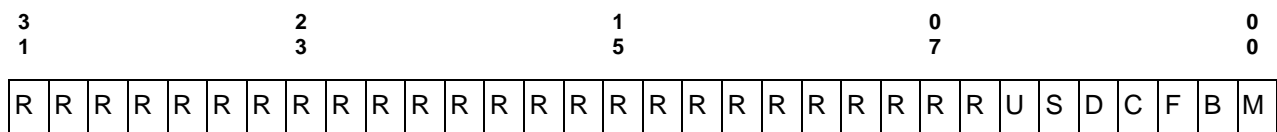
### 5.3.2.377 Visited Authorized Network Services

<b>Type</b>	377
<b>Length in octets</b>	1
<b>Value</b>	<p>4 octet Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 – CMIP4</li> <li>• Bit #1 – PMIP4</li> <li>• Bit #2 – Simple IPv4</li> <li>• Bit #3 – CMIP6</li> <li>• Bit #4 – PMIP6</li> <li>• Bit #5 – Simple IPv6</li> <li>• Bit #6 – Simple ETH Service</li> <li>• Bit #7 – MIP based ETH Service</li> <li>• Bit #8 – L2 DHCP Relay<sup>[a]</sup></li> </ul> <p>The rest of the bits are reserved</p>
<b>Description</b>	This TLV indicates whether V- and / or HCSN are authorized to anchor the ETH session or the IP session for Simple IP and PMIP services.
<b>Parent TLV</b>	MS Authorization Context

Note [a]: L2 DHCP Relay can be selected with either Simple ETH Service or MIP based ETH Service.

<b>Type</b>	436	
<b>Length in octets</b>	4	
<b>Value</b>	Compound	
<b>Description</b>	Data Integrity Compound TLV	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Data Integrity Method	O
<b>Parent TLV(s)</b>	MS Info	

<b>Type</b>	437
<b>Length in octets</b>	4
<b>Value</b>	<p>32-bit bitmask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 = M</li> <li>• Bit #1 = B</li> <li>• Bit #3 = F</li> <li>• Bit #4 = C</li> <li>• Bit #5 = D</li> <li>• Bit #6 = S</li> <li>• Bit #7 = U</li> </ul> <p>All other bits are Reserved.</p>
<b>Description</b>	This TLV is used to negotiate the Data Integrity Method. Each bit in the bitmask specifies one of the negotiable functionalities described in the section 4.7.7. The structure of the bitmask appears on the Figure 5-1.
<b>Parent TLV(s)</b>	Data Integrity Capability, SF Info



### Figure 5-1 – Structure of the Data Integrity Method bitmask

1

**Table 5-2 – Meanings of the bits**

Bit	Meaning	Notes
M	If set means per SF selected multi-unicasting will (or is offered to) be applied.	<p>The generic rule is the initiator of a transaction offers options and responder to the transaction selects options.</p> <p>Thus in Request messages all M, B and F bits may be set. In Response messages only one of them may be set.</p> <p>If none of these bits are set in the Response messages, then the HO data integrity feature SHALL NOT be supported for the handover.</p>
B	If set means Buffering at the Anchor DP will (or is offered to) be applied.	
F	If set means Per-SF S-BS Buffering and forwarding Data Integrity Method will be applied	
C	If set means Per-SF Bi-casting during the HO action phase will be applied.	This option can be set when the bit F is set to '1'. This option can be enabled also together with the option 'D'.
D	If set means BS to BS Data Path Establishment will be applied.	If set, it implies that R8 data path setup for Buffer Switching is supported by Target BS and Serving BS. This bit can be set only if bit F is set as well. If not set, the Data Integrity F will use R6, R4 data path for forwarding the data.
S	If set means ARQ Sync will (or is offered to) be applied.	Can be set independently of the other bits.
U	If set means Uplink Reassembly at Anchor DP will (or is offered to) be applied	Can be set only if S bit is set as well.
R	Reserved	

2

### 3 5.3.2.380 Data Integrity Applied

<b>Type</b>	438
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerated. The values are:</p> <ul style="list-style-type: none"> <li>0x00 = Not applied</li> <li>0x01 = Applied</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	This TLV is used to indicate whether the Data Integrity Method should be applied to a specific Service Flow or not.
<b>Parent TLV(s)</b>	SF Info

### 5.3.2.381 Pointer BSN

<b>Type</b>	439
<b>Length in octets</b>	2
<b>Value</b>	Internally structured 16-bit value
<b>Description</b>	The TLV Value occupies 2 octets of which 11 least significant bits denote BSN and the rest of the bits denote scope as shown on the Figure 5-2. The BSN points to the beginning or end of a region in a Block queue depending on the Scope value.
<b>Parent TLV(s)</b>	SF Info, SDU Info

Internal structure of the value field appears as follows:

15				11				07				04				00
Scope					BSN											

**Figure 5-2 – BSN TLV Value Field Format**

The Scope Values defined appear in the Table 5-3:

**Table 5-3 – Scope Values Defined**

<u>Scope Value</u>	<u>Description</u>
0	The BSN corresponds to the first Block in an SDU. In this case the Pointer BSN TLV should be included as sub-TLV of SDU Info.
1	Tx ARQ Window Start. In this case the Pointer BSN TLV should be included as sub-TLV of SF Info related to a downlink Service Flow.
2	Rx ARQ Window Start. In this case the Pointer BSN TLV should be included as sub-TLV of SF Info related to an uplink Service Flow.
3	Last BSN to Discard. Points to the BSN conveyed to the MS with the last Discard Message. All Blocks with BSNs lower than the specified are to be discarded. In this case the Pointer BSN TLV should be included as sub-TLV of SF Info related to a downlink Service Flow.
4	Last BSN to Purge. All Blocks with BSNs lower than and equal to the specified should be purged and acknowledged. In this case the Pointer BSN TLV should be included as sub-TLV of SF Info related to an uplink Service Flow.



### 5.3.2.382 BSN ARQ State Bitmap

<b>Type</b>	440
<b>Length in octets</b>	Variable: from 2 to 10
<b>Value</b>	Bitmask
<b>Description</b>	TLV is used to describe the Transmitter or Receiver BSN Queues for downlink or uplink Service Flows respectively. One TLV describes of up to 32 BSNs. The BSN field denotes the first BSN in the map, followed by up to 32 2-bit fields each of which denotes ARQ State of the contiguous Blocks starting with the one with the specified BSN. The Map Length field specifies how many 2-bit ARQ State fields are meaningful. One or more such TLVs might be included as sub-TLVs of SF Info. The structure of the value field appears on the Figure 5-3.
<b>Parent TLV(s)</b>	SF Info

The structure of the TLV:

00			03				07				11				15
BSN										Map Length					
ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St
ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St
ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St
ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St	ARQ St

**Figure 5-3 – BSN ARQ State Bitmap Format**

The meanings of the values of the ARQ St field are described in Table 5-4:

**Table 5-4 – ARQ State Values**

<u>Value</u>	<u>Meaning for Uplink SF</u>	<u>Meaning for Downlink SF</u>
0b00	Not Received State	Not Sent State
0b01	Ack Pending State	Outstanding
0b10	<i>Undefined.</i>	Waiting For Retransmission
0b11	Done State	Done State

1 **5.3.2.383 Switching Data Path ID**

<b>Type</b>	441
<b>Length in octets</b>	4
<b>Value</b>	Buffer Switching Data Path Identifier (e.g. GRE Key)
<b>Description</b>	Identifier for a buffer switching data path.
<b>Parent TLV(s)</b>	Data Path Info

2 **5.3.2.384 MAC Source Address and Mask**

<b>Type</b>	442
<b>Length in octets</b>	12
<b>Value</b>	A MAC Source Address/Mask pairs: (Src1, Smask) Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
<b>Description</b>	A MAC source address and mask. If this parameter is omitted, then comparison of the ethernet frame source address for this entry is irrelevant.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

3 **5.3.2.385 MAC Destination Address and Mask**

<b>Type</b>	443
<b>Length in octets</b>	12
<b>Value</b>	A MAC Destination Address/Mask pairs: (Dst1, Dmask) Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
<b>Description</b>	A MAC Destination address and mask. If this parameter is omitted, then comparison of the ethernet frame destination address for this entry is irrelevant.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

4 **5.3.2.386 ETYPE/SAP**

<b>Type</b>	444
<b>Length in octets</b>	3
<b>Value</b>	Ethernet Type or 802.2 SAP Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
<b>Description</b>	Ethernet Type or 802.2 SAP of the ethernet header.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

1 **5.3.2.387 User Priority Range**

<b>Type</b>	445
<b>Length in octets</b>	2
<b>Value</b>	User Priority Range:(User Priority Low, User Priority High) Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
<b>Description</b>	The value of the field specifies a range of user priority values in Ethernet frame header. If this parameter is omitted, user priority is irrelevant.
<b>Parent TLV</b>	Packet Classification Rule / Media Flow Description

2 **5.3.2.388 Void**

3 **5.3.2.389 Void**

4 **5.3.2.390 C-VID>S-VID Mapping**

<b>Type</b>	448
<b>Length in octets</b>	4
<b>Value</b>	C-VID,S-VID Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
<b>Description</b>	The value of the field specifies a mapping between a C-VID and a S-VID
<b>Parent TLV</b>	VLAN Tag Processing Rule

5 **5.3.2.391 C-VLAN Priority Setting**

<b>Type</b>	449
<b>Length in octets</b>	2
<b>Value</b>	Bitfield; the bits have the following meanings: <ul style="list-style-type: none"> <li>• 0x0000 = forward the p_bits without modification</li> <li>• 0x001x = drop frames with p_bits set to a higher value than x</li> <li>• 0x002x = set p_bits to x when p_bits set to a higher value than x</li> <li>• 0x003x = set the p_bits to x: insert VLAN tag with VLAN-ID=0 and p_bits set to value x into Ethernet frames without VLAN tag.</li> </ul> Other values reserved Note: One of the bitfield definitions can be assigned at a time.
<b>Description</b>	Defines the setting of the priority_bits in the C-VLAN tag in the upstream direction.
<b>Parent TLV</b>	VLAN Tag Processing Rule

### 1 5.3.2.392 VLAN ID Assignment

<b>Type</b>	450
<b>Length in octets</b>	2
<b>Value</b>	<p>Bitfield; the bits have the following meaning:</p> <ul style="list-style-type: none"> <li>• 0x0000 = forward VLAN tags without modification</li> <li>• 0x0010 = remove S-VID in downstream direction</li> <li>• 0x0020 = remove C-VID and S-VID, if present, in downstream direction</li> <li>• 0x010x = add C-VLAN tag in upstream to frames without C-VLAN tag with C-VID set to C-VLAN ID and p_bits set to x</li> <li>• 0x020x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set to S-VLAN ID and S-p_bits set to x</li> <li>• 0x0280 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set to S-VLAN ID and S-p_bits copied from C-p_bits</li> <li>• 0x040x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C-&gt;S-VID Mapping table and S-p_bits set to x If no entry exists for a particular C-VID in the C-VID&gt;S-VID Mapping table, the S-VID is set to 0</li> <li>• 0x0480 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C-&gt;S-VID Mapping Table and S-p_bits copied from C-p_bits If no entry exists for a particular C-VID in the C-VID&gt;S-VID Mapping table, the S-VID is set to 0</li> </ul> <p>Other values reserved</p> <p>Note: One downstream rule can be combined (ORed) with one upstream rule.</p>
<b>Description</b>	Defines the processing of the VLAN tags in both the upstream and downstream direction.
<b>Parent TLV</b>	VLAN Tag Processing Rule

### 2 5.3.2.393 SVLAN ID

<b>Type</b>	451
<b>Length in octets</b>	2
<b>Value</b>	<p>SVLAN ID</p> <p>Note: Encoding of the VLAN value follows section 11.13.18.3 of IEEE802.16-2009 [13].</p>
<b>Description</b>	The value of the field specifies a SVLAN ID.
<b>Parent TLV</b>	VLAN Tag Processing, Packet Classification Rule/Media Flow Descriptor

1 **5.3.2.394 CVLAN ID**

<b>Type</b>	452
<b>Length in octets</b>	2
<b>Value</b>	CVLAN ID Note: Encoding of the VLAN ID value follows section 11.13.18.3 of IEEE802.16-2009 [13].
<b>Description</b>	The value of the field specifies a CVLAN ID.
<b>Parent TLV</b>	VLAN Tag Processing, Packet Classification Rule/Media Flow Descriptor

2 **5.3.2.395 LocalConfigInfo**

<b>Type</b>	453
<b>Length in octets</b>	2+n
<b>Value</b>	String of length n containing arbitrary information The meaning of the information in LocalConfigInfo is subject of static configuration agreements between NAP and NSP.
<b>Description</b>	Local configuration information for preprovisioned R3 data path (Simple Ethernet)
<b>Parent TLV</b>	VLAN Tag Processing Rule

3 **5.3.2.396 VLANTagProcessingRuleID**

<b>Type</b>	454
<b>Length in octets</b>	2
<b>Value</b>	Short-Unsigned
<b>Description</b>	The value of the field provides a 16bit ID for the particular VLANTagProcessingRule. The value 0x0000 is reserved and indicates that no VLAN Tag Processing is performed for the particular service flow.
<b>Parent TLV</b>	VLAN Tag Processing Rule

### 1 5.3.2.397 VLAN Tag Processing Rule

<b>Type</b>	455	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Contains sub-elements representing the rules for processing the VLAN tags in the L2FW function in the case of ETH-CS. This TLV is valid only when the CS TYPE in SF INFO is ETH-CS.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	VLANTagProcessingRuleID	M
	VLAN Priority setting	M
	VLAN ID Assignment	O
	CVLAN ID	O
	SVLAN ID	O
	C-VID>S-VID Mapping	O <sup>1</sup>
	LocalConfigInfo	O <sup>2</sup>
<b>Parent TLV</b>	SF Info	

2 [1] This Sub-TLV MAY appear multiple times in the TLV

3 [2] LocalConfigInfo is not used in the case of MIP based Ethernet Services.

### 4 5.3.2.398 Uplink R3 GRE Key

<b>Type</b>	456
<b>Length in octets</b>	4
<b>Value</b>	Uplink GRE Key
<b>Description</b>	GRE key used to mark the uplink traffic on the R3 interface when GRE encapsulation is used over R3.
<b>Parent TLV</b>	MIP4 Info

### 5 5.3.2.399 Downlink R3 GRE Key

<b>Type</b>	457
<b>Length in octets</b>	4
<b>Value</b>	Downlink GRE Key
<b>Description</b>	GRE key used to mark the downlink traffic on the R3 interface when GRE encapsulation is used over R3.
<b>Parent TLV</b>	MIP4 Info

1 **5.3.2.400 Hotlining Context**

<b>Type</b>	458	
<b>Length</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Carries the Hotlining Context from PPC to HLD; if both are not Collocated.	
<b>Elements</b>	<b>TLV Name</b>	<b>M/O</b>
	R3 Hotline-Profile-ID	O
	R3 HTTP-Redirection-Rule	O
	R3 IP-Redirection-Rule	O
	R3 NAS-Filter-Rule	O
	R3 Hotline-Session-Timer	O
	R3 Hotline-Indication	O
	Remaining Hotline Session Timer	O
	Service-ID	O
<b>Message Primitives that Carries this TLV</b>	Hotlining Req, Hotlining Rsp	

2 **5.3.2.401 R3 Hotline-Profile-ID**

<b>Type</b>	459
<b>Length</b>	Octet String
<b>Value</b>	String representing a Hot-Line profile.
<b>Description</b>	ID to uniquely identify the user's Hot-Line profile. See 5.4.2.53 for more details.
<b>Parent TLV</b>	Hotlining Context

3 **5.3.2.402 R3 HTTP-Redirection-Rule**

<b>Type</b>	460
<b>Length</b>	Variable
<b>Value</b>	An string formatted as per IPFilterRule specified by RFC 3588 [54] with some exception: See 5.4.2.54 for more details.
<b>Description</b>	Instructs the Hot-Lining Device where to redirect HTTP flows.
<b>Parent TLV</b>	Hotlining Context

1 **5.3.2.403R3 IP-Redirection-Rule**

<b>Type</b>	461
<b>Length</b>	Variable
<b>Value</b>	An string formatted as per IPFilterRule specified by RFC 3588 [54] with some exception: See 5.4.2.55 for more details.
<b>Description</b>	Used to specify which packet flow to redirect and where to redirect it.
<b>Parent TLV</b>	Hotlining Context

2 **5.3.2.404R3 NAS-Filter-Rule**

<b>Type</b>	462
<b>Length</b>	Variable
<b>Value</b>	The String field is one or more octets.
<b>Description</b>	As defined by RFC 4849 [1]
<b>Parent TLV</b>	Hotlining Context

3 **5.3.2.405R3 Hotline-Session-Timer**

<b>Type</b>	463
<b>Length</b>	4
<b>Value</b>	Unsigned Integer representing a time in seconds. A value of zero means infinity.
<b>Description</b>	Specifies the length of time in seconds that the user would be allowed to remain in the Hot-Line session. See 5.4.2.56 for more details.
<b>Parent TLV</b>	Hotlining Context

4 **5.3.2.406 Remaining Hotline Session Timer**

<b>Type</b>	464
<b>Length</b>	4
<b>Value</b>	Unsigned Integer representing a time in seconds. A value of zero means infinity.
<b>Description</b>	Specifies the Remaining length of time in seconds that the user would be allowed to remain in the Hot-Line session. See 5.4.2.56 for more details.
<b>Parent TLV</b>	Hotlining Context

5 **5.3.2.407R3 Hotline-Indication**

<b>Type</b>	465
<b>Length</b>	Length of String
<b>Value</b>	A string value which is to be opaque.
<b>Description</b>	Indicates that the flow is Hot-Lined. See 5.4.2.24 for more details.
<b>Parent TLV</b>	Hotlining Context



### 1 5.3.2.408R3 Hotlining Capability

<b>Type</b>	466
<b>Length</b>	1
<b>Value</b>	Unsigned Integer.
<b>Description</b>	<p>Octet interpreted as a bit map with the following values:</p> <ul style="list-style-type: none"> <li>• Bit#0 = Profile-based Hot-Lining is supported (using the Hotline-Profile-ID VSA).</li> <li>• Bit#1 = Rule-based Hot-Lining is supported using NAS-Filter-Rule.</li> <li>• Bit#2 = Hot-Lining HTTP Redirection is supported.</li> <li>• Bit#3 = Rule-based Hot-Lining is supported using IP-Redirection rule.</li> </ul> <p>Other values reserved</p> <p>A value of zero (none of the bits being set) or the omission of this subTLV means that Hot-Lining is not supported.</p>
<b>Parent TLV</b>	R3 WiMAX Capability

### 2 5.3.2.409DSCP

<b>Type</b>	496
<b>Length</b>	1
<b>Value</b>	<p>Unsigned Octet representing the DSCP field as defined in RFC2474 [29]</p> <p>DSCP field as defined in rfc2475 [30]</p> <pre>       0   1   2   3   4   5   6   7 +---+---+---+---+---+---+---+---+             DSCP             CU   +---+---+---+---+---+---+---+ </pre> <p>DSCP: differentiated services codepoint CU: currently unused</p>
<b>Description</b>	<p>Differentiated services codepoint as defined in RFC 2474 [29]. <u>Used to mark the encapsulating IP packets of the flow on the R6 interface: BS marks the packets on the UL, ASN-GW marks the packets on the DL. (TOS bits of the encapsulated bearer packets are not changed by the ASN-GW or BS). The DSCP value is defined by the ASN-GW based on the local QoS policies (which may include keeping the AAA-provided value or over-writing it with the locally configured value).</u></p> <p>Used to mark the IP packets of the flow. See RFC3246 [46], RFC2597 [34] and RFC4595 [76] for recommended values.</p>
<b>Parent TLV</b>	QoS Parameters

### 5.3.2.410 PHY Mode ID

<b>Type</b>	497
<b>Length</b>	2
<b>Value</b>	A 16-bit value that specifies the PHY parameters, including channel bandwidth, FFT size, cyclic prefix, and frame duration, as specified in the IEEE802.16e [11].
<b>Description</b>	This TLV indicates which PHY mode SHALL be used at a BS. It SHALL be present in the message when the phy mode of a BS is different from the recipient BS, as defined in IEEE802.16e [11].
<b>Parent TLV</b>	RRM BS Info

### 5.3.2.411 Scheduling Service Supported

<b>Type</b>	498
<b>Length</b>	1
<b>Value</b>	8-bit bitmap, as specified in the IEEE802.16e [11].
<b>Description</b>	<p>This TLV indicates which scheduling service types can be supported at the BS.</p> <p>Bitmap to indicate if BS supports a particular scheduling service. 1 indicates support, 0 indicates not support:</p> <p>Bit #0: Unsolicited grant service (UGS)</p> <p>Bit #1: Real-time polling service (rtPS)</p> <p>Bit #2: Non-real-time polling service (nrtPS)</p> <p>Bit #3: Best effort (BE) service</p> <p>Bit #4: Extended real-time polling service (ertPS)</p> <p>Bits #5–7: Reserved; SHALL be set to zero.</p> <p>If the value of bit 0 through bit 4 is 0b00000, it indicates no information on service available.</p>
<b>Parent TLV</b>	RRM BS Info

### 5.3.2.412 PMIP6 Info

Type	425	
Length in octets	Variable	
Value	Compound	
Description	PMIP6 Information associated with the subscriber’s IP session.	
Elements (Sub-TLVs)	TLV Name	M/O
	LMA IPv6 Address	M
	Home Network Prefix (HNP)	O
	Home Address (HoA)	O
	LMA IPv4 Address	O
	PMIP6 Security Indicator	O
	MAG IPv6 Address	M

<b>Parent TLV(s)</b>	Anchor MM Context
----------------------	-------------------

1 **5.3.2.413 LMA IPv6 Address**

<b>Type</b>	426
<b>Length in octets</b>	16
<b>Value</b>	The Identifier in format of 16-octet IPv6 Address.
<b>Description</b>	IPv6 address of the LMA.
<b>Parent TLV(s)</b>	PMIP6 Info

2 **5.3.2.414 LMA IPv4 Address**

<b>Type</b>	427
<b>Length in octets</b>	4
<b>Value</b>	The Identifier in format of 4-octet IPv4 Address.
<b>Description</b>	IPv4 address of the LMA.
<b>Parent TLV(s)</b>	PMIP6 Info

3 **5.3.2.415 MAG IPv6 Address**

<b>Type</b>	428
<b>Length in octets</b>	16
<b>Value</b>	The Identifier in format of 16-octet IPv4 Address.
<b>Description</b>	IPv6 address of the LMA
<b>Parent TLV(s)</b>	PMIP6 Info

4 **5.3.2.416 Home Network Prefix (HNP)**

<b>Type</b>	429
<b>Length in octets</b>	0-16 octets
<b>Value</b>	Variable size IPv6 address prefix
<b>Description</b>	The IPv6 home network address prefix that is assigned to a MS for PMIP6 mobility
<b>Parent TLV(s)</b>	PMIP6 Info

5 **5.3.2.417 PMIP6 Security Indicator**

<b>Type</b>	430
<b>Length in octets</b>	1
<b>Value</b>	Indicates whether in-band signaling protection is used for PMIP6
<b>Description</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Lower-layer security</li> <li>• 0x01 = In-band security</li> </ul>
<b>Parent TLV(s)</b>	PMIP6 Info

1 **5.3.2.418DHCP Proxy Type**

<b>Type</b>	431
<b>Length in octets</b>	1
<b>Value</b>	Indicates IP version designation of the DHCP Proxy (IPv4 or IPv6)
<b>Description</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = DHCPv4 Proxy</li> <li>• 0x01 = DHCPv6 Proxy</li> </ul>
<b>Parent TLV(s)</b>	DHCP Proxy Info

2 **5.3.2.419PMIP6 Security Info**

Type	432	
Length in octets	Variable	
Value	Compound	
Description	PMIP6 security context and key	
Elements (Sub-TLVs)	TLV Name	M/O
	MAG-LMA-PMIP6 Key	O
	MAG-LMA-PMIP6 SPI	O
	MAG-LMA-PMIP6 Lifetime	O
Messages Primitive(s) that use this TLV	Anchor_DPF_Relocate_Rsp	

3 **5.3.2.420MAG-LMA-PMIP6 Key**

<b>Type</b>	433
<b>Length in octets</b>	20
<b>Value</b>	160-bit unsigned integer.
<b>Description</b>	The MAG-LMA-PMIP6 key used to calculate and authenticate AO in the PMIP6 PBU/PBA assures integrity and authorization of communicating MAG and LMA peers.
<b>Parent TLV(s)</b>	PMIP6 Security Info

4 **5.3.2.421 MAG-LMA-PMIP6 SPI**

<b>Type</b>	434
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Key ID of MAG-LMA-PMIP6 key. It should be equal to the SPI of PMIP6-RK.
<b>Parent TLV(s)</b>	PMIP6 Security Info

5 **5.3.2.422MAG-LMA-PMIP6-Lifetime**

<b>Type</b>	435
-------------	-----

<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Time for MAG-LMA-PMIP6 key remaining valid. This is provided to the MAG by the anchor Authenticator for PMIP6 key context transfer.
<b>Parent TLV(s)</b>	PMIP6 Security Info

1 **5.3.2.423 Mobility Access Classifier**

<b>Type</b>	499
<b>Length in octets</b>	1
<b>Value</b>	1 = Fixed 2 = Nomadic 3 = Mobile 4-255= Reserved
<b>Description</b>	This refers to the classification of the subscriber as fixed, nomadic, or mobile. Absence of this TLV means that MS is a mobile access subscriber.
<b>Parent TLV(s)</b>	MS Info, Information

2 **5.3.2.424 Reattachment Zone**

<b>Type</b>	500
<b>Length in octets</b>	Variable
<b>Value</b>	List of BS ID.
<b>Description</b>	BS ID List where a fixed or nomadic MS is allowed to reattach or handoff to.
<b>Parent TLV(s)</b>	BS Info, MS Info

3 **5.3.2.425 BS Location**

<b>Type</b>	501
<b>Length in octets</b>	Variable
<b>Value</b>	Octet String
<b>Description</b>	BS Location info which may be described as Lat/Long/Sector/carrier information of BS.
<b>Parent TLV(s)</b>	BS Info

4 **5.3.2.426 WiMAX Release Info**

Type	504		
Length in octets	Variable		
Value	Compound		
Description	Includes a WiMAX Release number plus an associated list of capability support indicator TLVs.		
Elements (Sub-TLVs)	TLV Name	M/O	
	R4R6R8 WiMAX Release	M	

	Capabilities Info	O
<b>Message Primitives That Use This TLV</b>	Capability_Req, Capability_Rsp, Capability_Ack	

1 **5.3.2.427 R4R6R8 WiMAX Release**

<b>Type</b>	505
<b>Length in octets</b>	Variable
<b>Value</b>	Octet string. A string indicating a WiMAX release formatted as: major + "." + minor. Same encoding as the "R3 WiMAX-Release" TLV in ASN control messages (section 5.3.2.441) and the "WiMAX Release" attribute in R3 RADIUS messages (section 0) and in R3 DIAMETER messages (section 5.5.2). For example, the first release of WiMAX is indicated as "1.0".
<b>Description</b>	Indicates the WiMAX Release number which is applied for the ASN control protocol signaling between two network nodes in the NAP network on R4, R6 and R8. Implementations compliant with this specification SHALL set the value to the string '1.5'.
<b>Parent TLV(s)</b>	WiMAX Release Info

2 **5.3.2.428 Capabilities Info**

<b>Type</b>	506	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	A list of optional capabilities supported by a network node for a given WiMAX Release.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Capabilities Negotiation Mode	M
	ASN-GW ROHC Capability (Note 1)	O
	Support-of-MCBCS	O
	Support-of-HO-DI	O
	Support-of-dMAC	O
	Support-of-OTA-DM	O
	Support-of-IMS-ES	O
	Support-of-PCC-QoS	O
	Support-of-EtherServ	O
	Support-of-LBS	O
	Support-of-FixedNom	O
	Support-of-NetRej	O
	Support-of-RRM	O
<b>Parent TLV(s)</b>	WiMAX Release Info	

- 1 Note: “ASN-GW ROHC Capability” is defined in the R1.5 ROHC Standalone Specification [8], section 7.3.2.7.

2 **5.3.2.429 Support-of-MCBCS**

<b>Type</b>	507
<b>Length in octets</b>	1
<b>Value</b>	0x00 = MCBCS is not supported 0x01 = MCBCS-DSx is supported 0x02 = MCBCS-Appl is supported All other values are Reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether MCBCS is supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

3 **5.3.2.430 Support-of-HO-DI**

<b>Type</b>	508
<b>Length in octets</b>	1
<b>Value</b>	0x00 = Handover Data Integrity is not supported 0x01 = Handover Data Integrity is supported All other values are Reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether Handover Data Integrity is supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

4 **5.3.2.431 Support-of-dMAC**

<b>Type</b>	509
<b>Length in octets</b>	1
<b>Value</b>	0x00 = Duplicate MS Context per MS MAC address is not supported 0x01 = Duplicate MS Context per MS MAC address is supported All other values are Reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether Duplicate MS Context per MS MAC address is supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

5 **5.3.2.432 Support-of-Accounting**

<b>Type</b>	510
<b>Length in octets</b>	1

<b>Value</b>	1 octet Bit Mask with the following values: 0x00 = No accounting. Only valid at the HA. 0x01 = IP/ETH-Session-based accounting. Default value for the ASN. 0x02 = Flow-based accounting. 0x04 = Flow-based accounting for ETH-CS. Remaining bits are reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates which accounting capabilities are supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

1 **5.3.2.433 Support-of-IMS-ES**

<b>Type</b>	511
<b>Length in octets</b>	1
<b>Value</b>	0x00 = IMS and Emergency Service is not supported 0x01 = IMS and Emergency Service is supported All other values are Reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether IMS and Emergency Service are supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

2 **5.3.2.434 Support-of-PCC-QoS**

<b>Type</b>	512
<b>Length in octets</b>	1
<b>Value</b>	0x00 = PCC-QoS is not supported 0x01 = PCC-QoS is supported All other values are Reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether PCC and dynamic QoS are supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

3 **5.3.2.435 Support-of-EtherServ**

<b>Type</b>	513
<b>Length in octets</b>	1
<b>Value</b>	0x00 = EtherServ is not supported 0x01 = EtherServ is supported All other values are Reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether Ethernet Service is supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info



1 **5.3.2.436 Support-of-LBS**

<b>Type</b>	514
<b>Length in octets</b>	1
<b>Value</b>	0x00 = LBS is not supported 0x01 = LBS is supported All other values are Reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether LBS is supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

2 **5.3.2.437 Support-of-FixedNom**

<b>Type</b>	515
<b>Length in octets</b>	1
<b>Value</b>	0x00 = FixedNom is not supported 0x01 = FixedNom is supported All other values are Reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether Fixed/Nomadic mobility restriction is supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

3 **5.3.2.438 Support-of-Hotlining**

<b>Type</b>	516
<b>Length in octets</b>	1
<b>Value</b>	1 octet Bit Mask with the following values: 0x00 = Hot-Lining is not Supported 0x01 = Profile-based Hot-Lining is supported (using the Hotline-Profile-ID VSA) 0x02 = Rule-based Hot-Lining is supported using NAS-Filter-Rule 0x04 = Hot-Lining HTTP Redirection is supported. 0x08 = Rule-based Hot-Lining is supported using IP-Redirection rule. Remaining bits are reserved.
<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates which Hot-Lining options are supported by the sending node.
<b>Parent TLV(s)</b>	Capabilities Info

4 **5.3.2.439 Support-of-RRM**

<b>Type</b>	517
<b>Length in octets</b>	1
<b>Value</b>	0x00 = RRM is not supported 0x01 = RRM is supported All other values are Reserved.

<b>Description</b>	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether RRM is supported by the sending node. (Note 1)
<b>Parent TLV(s)</b>	Capabilities Info

- 1 Note: Additional values might be used for indicating support for specific RRM procedures, e.g. Neighbor BS Status  
2 Update procedure or the Spare Capability reporting procedure.

### 3 5.3.2.440 R6\_Context\_ID

<b>Type</b>	572
<b>Length in octets</b>	12
<b>Value</b>	96 bit Unsigned Integer
<b>Description</b>	<p>Unique session identifier for an R6 context of a MS that is assigned by the BS and is used in the BS and Authenticator to separate parallel R6 messages for one or several MSes with the same MAC address during network entry. The R6_Context_ID is unique for all such contexts handled at a specific BS. Uniqueness across the ASN can be guaranteed in the Authenticator by using the combination of R6_Context_ID and BS_ID.</p> <p>The value '0' is reserved to indicate that no value is yet assigned and SHALL not be assigned by a BS as the R6_Context_ID.</p> <p>R6_Context_ID is placed after the message header according to the rules specified in section 3.2.</p>
<b>Parent TLV(s)</b>	None.

### 4 5.3.2.441 R3 WiMAX-Release

<b>Type</b>	573
<b>Length in octets</b>	Variable
<b>Value</b>	Octet String
<b>Description</b>	WiMAX release negotiated during Network Entry for the respective session.
<b>Parent TLV(s)</b>	R3 WiMAX Capability

5

### 5.3.2.442 Last Reset Time

<b>Type</b>	574
<b>Length in octets</b>	4
<b>Value</b>	The least significant 32-bits of Timestamp in UTC format.
<b>Description</b>	The timestamp of the last NE boot up. The NE generating this value SHOULD ensure the value is unique over the NE restarts.
<b>Parent TLV(s)</b>	Keep-alive Req, Keep-alive Rsp

### 5.3.2.443 Health Status

<b>Type</b>	575	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	This TLV is used to report the status of the peer or to report the status on behalf of other NE. The use of this TLV is FFS.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Status	M[a] [b]
	Reported Node ID	O [c]
	Reference Last Reset Time	O [d]
	Function ID	O [b]
<b>Message Primitives that use this TLV</b>	Keep-alive REQ	

Notes:

[a] Status TLV SHALL be always present in Health Status TLV.

[b] If Reported Node ID TLV is not present, the Status TLV and Function ID TLV are related to the originator of the message. If Reported Node ID TLV is present, the Status TLV and Function ID TLV are related to the corresponding reported NE.

[c] Reported Node ID TLV MAY be included to report status on behalf of other NE.

[d] If Reported Node ID TLV is included, Reference Last Reset Time TLV SHALL be also included.

1 **5.3.2.444 Status**

<b>Type</b>	576
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = Operating Normally</li> <li>• 0x01 = Failed</li> <li>• 0x02 = Shutting Down</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	The status of the message originator or the reported Network Entity as indicated by the presence of the Reported Node ID TLV.
<b>Parent TLV(s)</b>	Health Status

2 **5.3.2.445 Reported Node ID**

<b>Type</b>	577
<b>Length in octets</b>	Variable (could be of three fixed sizes: 4, 6 and 16 octets)
<b>Value</b>	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 ID value or 16-octet IPv6 Address. The length defines also the format of the Identifier.
<b>Description</b>	The Identity of the reported Network Entity.
<b>Parent TLV(s)</b>	Health Status

3 **5.3.2.446 Reference Last Reset Time**

<b>Type</b>	578
<b>Length in octets</b>	4
<b>Value</b>	The least significant 32-bits of Timestamp in UTC format
<b>Description</b>	The timestamp of the last boot up for the reported Network Entity. The use of this TLV is FFS.
<b>Parent TLV(s)</b>	Health Status

4 **5.3.2.447 Function ID**

<b>Type</b>	579
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator. The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = ALL (default)</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	Indicates the reported Functional Entity as defined for WiMAX ASN GW – Authenticator, Anchor GW or PC. If missing, the Default value is assumed.
<b>Parent TLV(s)</b>	Health Status

1 **5.3.2.448 ARQ Window Info**

<b>Type</b>	580	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	ARQ window information parameters which shall be used to deliver ARQ states of each SF at the Serving BS to the Target BS.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	Starting ARQ BSN	O
	Last ARQ BSN	O
	Valid ARQ BSN	O
	Reset Status	O
<b>Parent TLV(s)</b>	Data Path Info	

2 **5.3.2.449 Starting ARQ BSN**

<b>Type</b>	581
<b>Length in octets</b>	2
<b>Value</b>	16-bit Integer. Block Sequence Number, as defined in IEEE802.16e
<b>Description</b>	Identifies the Block Sequence Number of the first ARQ Block in the ARQ window of a particular SF.
<b>Parent TLV(s)</b>	ARQ Window Info

3 **5.3.2.450 Last ARQ BSN**

<b>Type</b>	582
<b>Length in octets</b>	2
<b>Value</b>	16-bit Integer. Block Sequence Number, as defined in IEEE802.16e
<b>Description</b>	Identifies the Block Sequence Number of the ARQ Block in the ARQ window of a particular SF, which is to be transmitted to (in case of downlink traffics) or received from (in case of uplink traffics) the MS after completion of the handover.
<b>Parent TLV(s)</b>	ARQ Window Info

4 **5.3.2.451 Valid ARQ BSN**

<b>Type</b>	583
<b>Length in octets</b>	2
<b>Value</b>	16-bit Integer. Block Sequence Number, as defined in IEEE802.16e
<b>Description</b>	This TLV indicates whether the ARQ Discard was outstanding at the Serving BS before HO indication from MS is received. If this TLV is included, the Target BS shall issue a ARQ_DISCARD MAC management message for Blocks, whose sequence numbers are less than or equal to the specified value, to the MS, right after the completion of MS HO.
<b>Parent TLV(s)</b>	ARQ Window Info

1 **5.3.2.452 Reset Status**

<b>Type</b>	584
<b>Length in octets</b>	1
<b>Value</b>	<p>Enumerator: The values are:</p> <ul style="list-style-type: none"> <li>• 0x00 = No ARQ RESET was issued at the Serving BS before HO</li> <li>• 0x01 = ARQ_RESET was outstanding at the Serving BS before HO</li> </ul> <p>All other values are Reserved.</p>
<b>Description</b>	This TLV indicates whether the ARQ Reset was outstanding at the Serving BS before HO indication from MS is received. If this TLV is set, the Target BS shall issue a ARQ_RESET MAC management message to the MS, right after the completion of MS HO.
<b>Parent TLV(s)</b>	ARQ Window Info

2 **5.3.2.453 HARQ Context**

<b>Type</b>	585	
<b>Length in octets</b>	Variable	
<b>Value</b>	Compound	
<b>Description</b>	Contains HARQ related information for the service flow. If TLV is missing, then HARQ is disabled in the service flow.	
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>M/O</b>
	HARQ Enable	O
	HARQ Channel Mapping	O
	PDU SN extended subheader for HARQ reordering	O
<b>Parent TLV(s)</b>	SF Info, SBC Context	

3 **5.3.2.454 HARQ Enable**

<b>Type</b>	586
<b>Length in octets</b>	1
<b>Value</b>	This TLV is received over the R1 interface and shall follow the 802.16e definition.
<b>Description</b>	As defined in IEEE802.16e. If TLV is missing, then HARQ is disabled in the service flow.
<b>Parent TLV(s)</b>	HARQ Context

4 **5.3.2.455 HARQ Channel Mapping**

<b>Type</b>	587
<b>Length in octets</b>	1
<b>Value</b>	This TLV is received over the R1 interface and shall follow the 802.16e definition.
<b>Description</b>	As defined in IEEE802.16e. If TLV is missing, then all HARQ channels are used in the service flow.
<b>Parent TLV(s)</b>	HARQ Context

1 **5.3.2.456 PDU SN extended subheader for HARQ reordering**

<b>Type</b>	588
<b>Length in octets</b>	1
<b>Value</b>	This TLV is received over the R1 interface and shall follow the 802.16e definition.
<b>Description</b>	As defined in IEEE802.16e. If TLV is missing, then PDU SN is not used in the service flow.
<b>Parent TLV(s)</b>	HARQ Context

## 5.4 RADIUS Messages and Attributes

The section lists the standard attributes that are used across RADIUS-based WiMAX reference points, and all VSAs (vendor-specific attributes) that are defined for WiMAX network operation as describe by this specification.

### 5.4.1 RADIUS Messages

#### 5.4.1.1 Network Access Authentication between NAS and HAAA

The RADIUS attributes defined in the following tables, comprise:

- attributes used for EAP-based network access that are exchanged between the ASN and the HAAA in the CSN.
- additional attributes for bootstrapping mobility service that are exchanged between ASN and the CSN HAAA.
- RADIUS attributes between ASN and HAAA for DHCP relay.

### RADIUS Attribute Tables

**Table 5-5 – 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-Identity).	1	0	0-1[aa]	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 [52] in an Access-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	0-1[m]	0	0-1[m]	0



Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
		bytes (the recommended value is 1400 bytes)." In an Access-Accept the use is as per [37].				
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 [52].	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	1	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 of the device as a 17 byte Upper Case ASCII value as defined by RFC 3580 sec 3.21 and 802-2001 in canonical order. For example "00-10-A4-23-19-C0" is Valid and 00-10-a4-23-19-c0 is not valid; and 00:10:A4:23:19:C0 is not valid.	1	0	0	0
CUI	89	Indication for support and desire to have the HAAA provide Chargeable User Identity. The NAS commits to include the CUI in all	0-1	0	0-1[a]	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
		RADIUS Accounting packets.				
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 [51].	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]	0
Framed-IP-Address	8	The IP4 address assigned to the MS by HCSN.	0	0	0-1[c]	0
Visited-Framed-IP-Address	26/79	The IP4 address assigned to the MS by VCSN.	0-1[t]	0	0-1[t]	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 (i.e., MSK, EMSK and keys derived from EMSK). Session-Timeout in an Access-Challenge packet is used set the EAP-retransmission timer as per [52].	0	0-1	0-1[d]	0
Termination-Action	29	Indicates what action the NAS should take when service is completed.	0	0	0-1[d]	0
WiMAX-Session-Id	26/4	A unique identifier in the home realm for this Session as set by the HAAA.	0-1[e]	0-1	1	0
MSK	26/5	The Master Session Key derived as the result of successful EAP Authentication.	0	0	0-1[f]	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Packet-Flow-Descriptor	26/28	The pre-provisioned Service Flows. (This Attribute is deprecated in this release).	0	0	0[x]	0
Packet-Flow-Descriptor-V2	26/84	The pre-provisioned Service Flows	0	0	1-n	0
QoS-Descriptor	26/29	The QoS descriptor for the pre-provisioned flows.	0	0	0-n[j]	0
VLANTagProcessing-Descriptor	26/211	The VLANTagProcessing descriptor for the pre-provisioned flows	0	0	0-n[u]	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
BS-Location	26/88	May be used as an alternative Serving BS identifier and usually indicates the location information of the BS which may be described as Lat/Long/Sector/Carrier information of the serving BS.	0-1	0	0	0
Mobility-Access-Classifer	26/89	Indicates the classification of the subscriber at the H-AAA as a fixed, nomadic or mobile access subscriber.	0	0	0-1	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	0
NSP-ID	26/57	The Operator ID of the NSP.	0-1[p]	0	0	0
Time-Of-Day-Time	26/20	The tariff time change for volume billing and duration billing.	0	0	0-n	0
PMIP-Authenticated-	26/78	The Proxy Mobile IP identity allocated by the	0-1[y]	0	0-1	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Network-Identity		network after Authentication.				
DNS	26/52	The IPv4/IPv6 address of the DNS server.	0	0	0-n[r]	0
State	24	A magic cookie to be returned along with user's response.	0-1[s]	0-1[s]	0-1[s]	0
Framed-IPv6-Prefix	97	Unique prefix to be assigned to the MS by Home CSN.	0	0	0-1	0
Framed-Interface-Id	96	The IPv6 interface id assigned by the Home CSN to be used for the MS. Used only for DHCPv6-based address configuration.	0	0	0-1	0
Visited-Framed-IPv6-Prefix	26/80	The unique prefix assigned to the MS by Visited CSN.	0-1[t]	0	0-1[t]	0
Visited-Framed-Interface-Id	26/81	The IPv6 interface id assigned by the visited CSN to be used for the MS. Used only for DHCPv6-based address configuration.	0-1[t]	0	0-1[t]	0
MS-Authenticated	26/90	Indication that MS has successfully performed device authentication	0	0	0-1	0
Operator-Name	To be assigned by IETF	Operator-Name contains the Visited NSP's WRI-Code in the Access-Request and Home NSP's WRI-Code in the Access-Accept	0-1[v]	0	0-1[w]	0
Certified-MS-Feature-List-For-GW	26/139	List of MS Certified features relevant for the ASN-GW policy for this MS.	0	0	0-1[z]	0
Certified-MS-Feature-List-For-BS	26/140	List of MS Certified features relevant for the BS policy for this MS.	0	0	0-1[z]	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 attribute for PMIP case. If this attribute is absent then the Home Address is derived from MIP procedures or other means (e.g., DHCP).
- [d] 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 packet. SHALL be included in all subsequent Access-Requests message for this session if known by the NAS.
- [f] The attribute SHALL be encrypted using the procedures in section 3.5 of [39]. MSK may be transmitted using MS\_MPPE\_Send\_Key and MS\_MPPE\_Recv\_Key as per [32] in which case MSK SHALL NOT appear in the Access-Accept packet.
- [g] Intentionally not used.
- [h] If more than one Class attribute is found in an Access-Accept packet, the NAS SHALL only store the first one and discard the rest.
- [i] Intentionally not used.
- [j] Conditional mandatory: see requirements for Packet Flow Descriptor.
- [k] Intentionally not used.
- [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 [52] 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.
- [q] Void.
- [r] If more than one DNS server IP address is given, then the first one is the primary and the others are secondary servers. DNS Server IP address is optional only for the case where WiMAX Capability negotiation for support of DHCP Relay is successful. At least one DNS Server IP address SHALL be present if WiMAX Capability negotiation for support of DHCP Relay is failed or not supported.
- [s] This Attribute is available to be sent by the server to the client in an Access-Challenge and MUST be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any. It SHALL be included in Access-Accept packets that have no CHAP password, user password or EAP message. Such as those with “service-type” = “authorize-only”.
- [t] In an Access-Request, this attribute is present between VAAA and HAAA only when VAAA wants to propose IP-address. If HAAA allows Visited network to assign IP address, it echoes back the IP address in Access-Accept to VAAA, and VAAA forwards it to the NAS. If IP address assignment by Visited network is not allowed the HAAA SHALL remove the Visited-framed-IP-address, and sends Framed-IP-Address.  
  
If the Framed-IP-address from both VCSN and HCSN is available in an Access-Accept, then an anchor selection mechanism needs to be executed by the NAS to select the anchor CSN for the data path. The details of this mechanism are outside the scope of this specification.
- [u] Conditional mandatory: see requirements for Packet Flow Descriptor.
- [v] SHALL NOT be added to the Access-Request by the NAS. If added, it SHALL be added by the VNSP.

- [w] The HAAA SHALL include this attribute set with its WRI-Code if the Operator-Name attribute was included in the Access-Request.
- [x] Support of Packet-Flow-Descriptor is deprecated in this release and only Packet-Flow-Descriptor V2 SHALL only be used instead.
- [y] SHALL not be included in the initial Access-Request message. MAY be included in subsequent Access-Requests message for this session if received by NAS from AAA.
- [z] SHALL be present if CRN is received as part of NAI decoration.
- [aa] WiMAX Forum is considering a future revision to change the multiplicity to 0 as the IETF RFC does not clarify what the NAS should do if User-Name is specified in Access-Accept.

Table 5-7 and Table 5-8 are the Mobility attributes exchanged between the ASN and the HAAA during the Network Access Authentication.

**Table 5-6 – RADIUS COA Messages between NAS and HAAA**

Attribute	TYPE	Description	COA	COA-ACK	COA-NAK
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [52]	1	1	1
Error-Cause	101	Error Codes generated during access authentication [51]	0	0	0-1
WiMAX-Session-Id	26/4	A unique identifier in the home realm for this Session as set by the HAAA.	1[b]	1[b]	0
Packet-Flow-Descriptor	26/28	The pre-provisioned Service Flows	0[d]	0	0
Packet-Flow-Descriptor-v2	26/84	The pre-provisioned Service Flows	0-n	0	0
QoS-Descriptor	26/29	The QoS descriptor for the pre-provisioned flows	0-n[a,c]	0	0

**Notes:**

- [a] Conditional mandatory: see requirements for Packet-Flow-Descriptor.
- [b] WiMAX-Session-Id which is equal to the Acct\_Multi\_Session-ID SHALL be used in Access-Accept packet if NAS supports Acct\_Multi\_Session-ID.
- [c] The complete QoS-profile must be transferred as the original context in ASN will be replaced. See the description of Packet Flow Descriptor for further details.
- [d] Support of Packet-Flow-Descriptor is deprecated in this release. Packet-Flow-Descriptor-V2 SHALL only be used instead.

**Table 5-7 – RADIUS Messages between ASN and HAAA for Bootstrapping Mobility Service**

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
hHA-IP-MIP4	26/6	IPv4 address of the home HA. To be used by the MIP4 client	0-1[a1]	0	0-1 [a9] [a11]	0
vHA-IP-MIP4	26/64	IPv4 address of the visited HA. To be used by the PMIP4 client.	0	0	0-1 [a2] [a11]	0
hHA-IP-MIP6	26/7	IPv6 address of the home HA. To be delivered to the MN via DHCP.	0-1[a9]	0	0-1 [a9] [a11]	0
vHA-IP-MIP6	26/65	IPv6 address of the visited HA. To be delivered to the MN via DHCP.	0-1[a9]	0	0-1 [a2] [a11]	0
MN-hHA-MIP4-KEY	26/10	The MN-hHA key used for Proxy MIP4 procedures.	0	0	0-1 [a9]	0
MN-vHA-MIP4-KEY	26/66	The MN-vHA key used for Proxy MIP4 procedures.	0	0	0-1 [a2]	0
MN-hHA-MIP4-SPI	26/11	The SPI associated with the MN-hHA-MIP4-KEY.	0	0	0-1 [a5]	0
MN-vHA-MIP4-SPI	26/71	The SPI associated with the MN-vHA-MIP4-KEY.	0	0	0-1 [a2]	0
FA-RK-KEY	26/14	The FA-RK used to derive MN-FA for MIP4 operations.	0	0	1	0
FA-RK-SPI	26/61	The SPI associated with the FA-RK.	0	0	1	0
hHA-RK-KEY	26/15	hHA-RK key used to generate FA-HA keys for MIP4 operations.	0	0	0-1 [a8]	0
hHA-RK-SPI	26/16	The SPI associated with the hHA-RK.	0	0	0-1 [a6] [a8]	0
hHA-RK-Lifetime	26/17	hHA-RK key lifetime.	0	0	0-1 [a6] [a8]	0

vHA-RK-KEY	26/67	vHA-RK key used to generate FA-HA keys for MIP4 operations.	0	0	0-1 [a11]	0
vHA-RK-SPI	26/68	The SPI associated with vHA-RK.	0	0	0-1 [a6] [a10]	0
vHA-RK-Lifetime	26/69	vHA-RK key lifetime.	0	0	0-1 [a6] [a10]	0
Framed-IPv6-Prefix	97	Unique prefix to be assigned to the MS.	0	0	0-1 [a3] [a7]	0
PMIP6-Service-Info	26/126	Indicates which PMIP6 protocol features are supported / authorized.	0-1	0	0-1[a12]	0
hLMA-IPv6-PMIP6	26/127	IPv6 address of the LMA in the HCSN	0	0	0-1[a13]	0
hLMA-IPv4-PMIP6	26/128	IPv4 address of the LMA in the HCSN	0	0	0-1	0
vLMA-IPv6-PMIP6	26/129	IPv6 address of the LMA in the VCSN	0-1	0	0-1[a13]	0
vLMA-IPv4-PMIP6	26/130	IPv4 address of the LMA in the VCSN	0-1[a15]	0	0-1	0
PMIP6-RK-KEY	26/131	PMIP6 root key used for ASN's key derivation	0	0	0-1	0
PMIP6-RK-SPI	26/132	SPI associated with PMIP6 root key	0	0	0-1	0
Home-HNP-PMIP6	26/133	Unique per-MS IPv6 prefix allocated from HCSN for PMIP6	0	0	0-1	0
Home-Interface-Id-PMIP6	26/134	IPv6 interface id for PMIP6 DHCPv6 mode	0	0	0-1[a14]	0
Home-IPv4-HoA-PMIP6	26/135	IPv6 HoA from HCSN for PMIP6-IPv4 MS	0	0	0-1	0
Visited -HNP-PMIP6	26/136	Unique per-MS IPv6 prefix allocated from VCSN for PMIP6	0	0	0-1	0
Visited -Interface-Id-PMIP6	26/137	IPv6 interface id for PMIP6 DHCPv6 mode	0	0	0-1	0
Visited -IPv4-HoA-PMIP6	26/138	IPv6 HoA from VCSN for PMIP6-IPv4 MS	0	0	0-1[a14]	0

1 **Notes:**

- [a1] This attribute MAY be included to propose the MIP4 address of the HA for the session. This attribute, and not the vHA-IP-MIP4 attribute, is used here for backwards compatibility.



- [a2] If the HAAA authorizes the visited HA assignment, then the HAAA SHALL include this attribute. In the case of the vHA-IP-MIP4 attribute, its value SHALL be set to the value received in the hHA-IP-MIP4 attribute in the associated Access-Request. In the case of the vHA-IP-MIP6 attribute, its value SHALL be set to the value received in the vHA-IP-MIP6 attribute in the associated Access-Request.
- [a3] Intentionally not used.
- [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 associated HA-RK is present. If they are not present the receiver SHALL ignore the HA-RK attribute.
- [a7] This attribute SHALL be assigned by the AAA server located in the CSN that is directly connected to the ASN.
- [a8] If the hHA-IP-MIP4 attribute is present, then this attribute SHALL be present.
- [a9] If the HAAA does not provide an HA assignment in the home network, then this attribute SHALL NOT be included.
- [a10] These attribute SHALL be provided by the VAAA if the HA is assigned in the visited network indicated by the presence of the vHA-IP-MIP4 attribute.
- [a11] If both, HA assignment at home network and HA assignment at the visited network are allowed by the HAAA, then this attribute SHALL be included. An HA selection mechanism needs to be executed by the NAS to select which HA will anchor the mobility session. The details of this mechanism are outside the scope of this specification.
- [a12] This attribute SHALL be included in Access-Accept when PMIP6 is among the Authorized Network services
- [a13] When PMIP6 is an Authorized Network service, either Home- or Visited LMA IPv6 address SHALL be present in the Access-Accept.
- [a14] This attribute SHALL be included by the HAAA when DHCP Proxy mode with preconfigured HNP is authorized.
- [a15] This attribute SHALL be included by the VAAA when LMA with IPv4 support is offered as PMIP6 anchor in the VCSN, and when IPv4-based R3 between ASN and VCSN is available.

1

**Table 5-8 – RADIUS Attributes between ASN and HAAA for DHCP Relay**

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
hDHCPv4-Server	26/8	The IPv4address of the home DHCP.	0	0	0	0
vDHCPv4-Server	26/73	The IPv4address of the visited DHCP server.	0-1[a1]	0	0-1[a2]	0
hDHCPv6-Server	26/9	The IPv6 address of the home DHCP-Server.	0	0	0	0
vDHCPv6-Server	26/74	The IPv6 address of the visited DHCP-Server.	0-1[a1]	0	0-1[a2]	0

hDHCP-RK	26/40	hDHCP-RK key used to derive keys to protect DHCP signaling between the DHCP relay and the home DHCP server.	0	0	0-1	0
vDHCP-RK	26/75	vDHCP-RK key used to derive keys to protect DHCP signaling between the DHCP relay and the visited DHCP server.	0	0	0-1 [a5]	0
hDHCP-RK-Key-ID	26/41	Key identifier associated with the hDHCP-RK, as per [65].	0	0	0-1 [a4]	0
vDHCP-RK-Key-ID	26/76	Key identifier associated with the vDHCP-RK, as per [65].	0	0	0-1 [a5][a4]	0
hDHCP-RK-Lifetime	26/42	Lifetime of the hDHCP-RK.	0	0	0-1 [a4]	0
vDHCP-RK-Lifetime	26/77	Lifetime of the vDHCP-RK.	0	0	0-1 [a5][a4]	0
hDHCP-Server-Parameters	26/86	Home DHCP server and corresponding security keys.	0	0	0-n[a7]	0
vDHCP-Server-Parameters	26/87	Visited DHCP server and corresponding security keys.	0-n[a8]	0	0-n[a8]	0

1 **Notes:**

- [a1] The VCSN MAY include the vDHCPv4-Server attribute or vDHCPv6-Server attribute to indicate that it is capable of assigning a DHCP server for the session. If the VCSN includes the vDHCPv4-Server attribute then it SHALL also include the HA-IP-MIP4 attribute. If multiple vDHCP-Servers are to be sent the first one will be present in this attribute and the rest will be present in vDHCP-Server-Parameters (26/87) attributes.
- [a2] If the Home AAA includes this attribute, the visited/proxy AAA may assign it.
- [a3] Intentionally not used.
- [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 the vAAA assigns the vDHCP it SHALL include this attribute.
- [a6] If Multiple hDHCP-Servers are present the first one will be present in this attribute and the rest will be present in hDHCP-Server-Parameters (26/86).
- [a7] If more than one hDHCP-Server is sent then the first one will be present in hDHCPv4-Server (26/8) or hDHCPv6-Server (26/9) attribute and the rest will be present in hDHCP-Server-Parameters(26/86) attributes.
- [a8] If more than one vDHCP-Server is sent then the first one will be present in vDHCPv4-Server (26/73) or vDHCPv6-Server (26/74) attribute and the rest will be present in vDHCPv4-Server-Parameters(26/87) attributes.

#### 5.4.1.2 RADIUS Messages for MIP between HA/LMA and HAAA

Table 5-9 shows the RADIUS attributes exchanged between the HA and HAAA. The HA always sends RADIUS messages to a AAA server that is located in the same CSN as the HA itself, in order to communicate with the HAAA server.

**Table 5-9 – RADIUS Messages between HA and HAAA**

Attribute	TYPE	Description	Access Request	Access Challenge	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
Class	25	Opaque value set by the Server used to bind authentication to accounting.	0	0	0-1[n]	0
WiMAX-Capability	26/1	Identifies the WiMAX Capabilities supported by the HA. Indicates capabilities selected by the RADIUS server.	1	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
WiMAX-Session-Id	26/4	A unique identifier in the home realm for this Session as set by the HAAA.	0-1[d]	0	1	0

Attribute	TYPE	Description	Access Request	Access Challenge	Access Accept	Access Reject
hHA-IP-MIP4	26/6	The IP address of the home 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	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.	0-1[m]	0	0-1[k]	0
MN-HA-MIP6-SPI	26/13	The SPI associated with the MN-HA-MIP6-KEY.	0-1[m]	0	0-1[k]	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[j]	0	0-1[h]	0
HA-RK-Lifetime	26/17	HA-RK Lifetime	0	0	0-1[h]	0
MIP-Authorization-Status	26/82	Indicates whether the MS is authorized to use MIP6.	0	0	0-1[i]	0
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	0	0	0-1	0

Attribute	TYPE	Description	Access Request	Access Challenge	Access Accept	Access Reject
		for this specific session.				
WiMAX-DM-Action-Code	26/60	Indicates that CMIP6 MS registered a new care-of address.	0-1[l]	0	0	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 MN-HA-MIP4-KEY or MN-HA-MIP6-KEY included in the message.	0	0	0-1[o]	0

1 **Notes:**

- [a] SHALL be included if the HA-IP address in the MIP RRQ is different than 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. For additional detail refer to sections 4.8.2.1.5 and 4.8.2.1.6.
- [d] WiMAX 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 WiMAX-Session-Id. For additional detail refer to sections 4.8.2.1.5 and 4.8.2.1.6.
- [e] In Access-Accept the MN-HA-SPI SHALL be present if it is different than the MN-HA-SPI received in the Access-Request.
- [f] The hHA-IP-MIP4 SHALL be present in an Access-Request. Note, the HA does not know whether it is in the Home or Visited domain, so defaults to assuming Home domain.
- [g] If the MN-HA-MIP4-SPI or MN-HA-MIP6-SPI is present in the Access-Request, then 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 packet. However, when present, all of the attributes SHALL be present otherwise the receiver SHALL silently discard the Access-Accept. And these attributes SHALL be filled by the local AAA server, which belongs to the same NSP with HA.
- [i] SHALL be present if this is associated with MIP6 procedures.
- [j] SHALL be present and should be set to the same FA-HA SPI value received from MIP RRQ if the HA need HA-RK-Key.
- [k] Either MN-HA-MIP4-SPI or MN-HA-MIP6-SPI SHALL be included if the associated MN-HA key is included.
- [l] SHALL be present in case of CMIP6 handover as described in section 4.8.4.2.
- [m] This attribute SHALL be present in the request when the associated MN-HA key is requested.
- [n] If more than one Class attribute is found in an Access-Accept packet, the HA SHALL only store the first

one and discard the rest.

- [o] Session-Timeout SHALL be present in Access-Accept if the associated MN-HA key is present in Access-Accept. If Termination-Action is present it SHALL be set to “DEFAULT”(0). This causes the HA to terminate the binding when the Session-Timeout expires.

Table 5-10 shows the RADIUS attributes exchanged between the LMA and HAAA. The LMA always sends RADIUS messages to a AAA server that is located in the same CSN as the LMA itself, in order to communicate with the HAAA server.

**Table 5-10 – RADIUS Messages between LMA and HAAA**

Attribute	TYPE	Description	Access Request	Access Challenge	Access Accept	Access Reject
User-Name	1	NAI extension received in the PMIP6 PBU.	1	0	0	0
NAS-IP-Address	4	The IP Address of the LMA's interface to the AAA server.	0-1[a]	0	0	0
NAS-IPv6-Address	95	The IPv6 Address of the LMA's interface to the AAA server.	0-1[a]	0	0	0
NAS-Identifier	32	The FQDN of the LMA's interface as seen by the AAA server.	1[a]	0	0	0
NAS-Port-Type	61	The absence of the NAS-Port-Type and presence of the PMIP6 attributes indicates that the message is coming from a LMA.	0	0	0	0
Message-Authenticator	80	Message Authenticator to integrity protect the AAA message.	1	0	1	0
Class	25	Opaque value set by the Server used to bind authentication to accounting.	0	0	0-1[b]	0
WiMAX-Capability	26/1	Identifies the WiMAX Capabilities supported by the LMA. Indicates capabilities selected by the RADIUS server.	1	0	1	0
CUI	89	Chargeable User Identity. It is a unique temporary handle to the user responsible for paying the bill.	0-1[d]	0	0-1[d]	0
WiMAX-	26/4	A unique identifier in the	0-1[d]	0	1	0

Attribute	TYPE	Description	Access Request	Access Challenge	Access Accept	Access Reject
Session-ID		home realm for this Session as set by the HAAA.				
Acct-Interim-Interval	85	Indicates the number of seconds between each interim update in seconds for this specific session.	0	0	0-1	0
PMIP6-Sservice-Info	26/126	Indicates PMIP6 protocol features that are supported by the LMA, and those authorized by AAA server	0-1[f]	0	0-1[f]	0
PMIP6-RK-KEY	26/131	PMIP6 root key used for LMA's key derivation	0	0	0-1	0
PMIP6-RK-SPI	26/132	SPI associated with PMIP6 root key	0-1	0	0-1	0
Home-HNP-PMIP6	26/133	HNP received in the PBU or authorized by the AAA	0-1	0	0-1	0
Home-IPv4-HoA-PMIP6	26/135	IPv4-HoA received in the PBU or authorized by the AAA	0-1	0	0-1	0
Session-Timeout	27	The maximum number of seconds of service. Associated with the lifetime of the PMIP6-RK included in the message for the MAG-LMA-PMIP6 key.	0	0	0-1[g]	0

1 **Notes:**

- [a] NAS-Identifier is required. Either NAS-IP or NAS-IPv6 MAY also be provided.
- [b] If more than one Class attribute is found in an Access-Accept message, the HA SHALL only store the first one and discard the rest.
- [c] With respect to release discovery, if the HAAA does not include the WiMAX-Capability in the Access-Accept packet, the receiver (LMA) SHALL assume that the release supported by the HAAA is the release that it proposed in the WiMAX-Capability sent in the Access-Request packet. In this case PMIP6 will not be triggered and the incoming PBU SHALL be rejected.
- [d] 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.
- [e] WiMAX 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 WiMAX-Session-ID.
- [f] SHALL be present if the AAA request/response is associated with PMIP6 procedure. If attribute is missing from Access-Accept, the LMA will not trigger PMIP6 and SHALL reject the incoming PBU.
- [g] Session-Timeout SHALL be present if the associated PMIP6-RK is included. If the Termination-Action is present its value SHALL be set to DEFAULT (0). This causes the LMA to terminate the binding when the

session timeout expires

### 5.4.1.3 RADIUS Messages between DHCP and HAAA

Table 5-11 defines the RADIUS messages that are exchanged between a DHCP server and the HAAA.

**Table 5-11 – 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

#### 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.



#### 5.4.1.4 RADIUS Message for Hot-Lining

Table 5-12 describes the RADIUS attributes sent from the HAAA to the Hot-Line Device (NAS or the HA).

**Table 5-12 – 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 Hot-Line 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	92	As defined by RFC 4849.	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

#### 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 [37] SHALL NOT be include in the RADIUS packet. A RADIUS packet that violates this rule SHALL be discarded.

Table 5-13 lists the RADIUS attributes that appear in a COA message used to Hot-Line the MS mid-session. The procedures for sending COA messages as described in [51] are supported with the additional information as specified by this table.

**Table 5-13 – 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. The NAI SHALL be formatted as received by the AAA server in Access-Request.	1	0	0

Attribute	TYPE	Description	COA	COA-ACK	COA-NAK
Calling-Station-Id	31	The MAC address in binary format of the MS.	1	0	0
WiMAX-Session-Id	26/4	The NAI contained in the User-Name and the WiMAX-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	92	As defined by RFC 4849.	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 [37] SHALL NOT be include in the RADIUS packet. A RADIUS packet that violates this rule SHALL be discarded.

2

#### 5.4.1.5 Messages for Online-Accounting

Online-Accounting message happen during Network Access Authentication and mid-session to update quotas. The 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

#### 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] MAY 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. This attribute SHOULD NOT be included as the NAS is required to support this capability, and inclusion therefore serves no additional purpose.
- [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 packet contains a PTS attribute or the PPAC "Tariff Switching supported" flag is set, it SHALL also contain an Event-Timestamp RADIUS attribute (see [40]).

### 1 5.4.1.6 Offline Accounting

#### 2 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]
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
Beginning-of-Session	26/22	True: a new flow is starting. False or missing, this is a continuation of a previous flow.	0-1	0	0
Network-Technology	26/23	Proxy CMIP4, CMIP4, Simple IP4, Simple IP6, CMIP6, Simple ETH, MIP based ETH and PMIPv6.	0-1[5]	0-1[5]	0-1[5]
Hotline-Indication	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	26/59	Unsigned Octet value used to indicate if the record represents compressed counts over-the-air. <ul style="list-style-type: none"> <li>0x00 = Uncompressed counts</li> <li>0x01 = Compressed counts</li> </ul>	0	1	1
NAS-Port-Type	61	Identifies the type of port (ASN or HA) the accounting record is associated with.	0-1[6]	0-1[6]	0-1[6]
MCBCS-Service-Type	111	Indicates the type of MCBCS service (e.g. streaming, download etc.). See [9] for the AVP definition.	1[7]	0-1[7]	0-1[7]
Transport-Type	112	Indicates the type of transport used to deliver content. See [9] for the AVP definition.	1[7]	0-1[7]	0-1[7]

### 3 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.
- [6] In accounting messages generated from the ASN, the NAS-Port-Type SHOULD be included and set to 27

for “Wireless – IEEE 802.16” when coming from a WiMAX ASN. Accounting message coming from an HA SHALL omit this attribute. If the home AAA is not sure whether this attribute is supported as per the above recommendation, then the home AAA can use the Class attribute to help it identify the source of the accounting messages.

[7] This attribute is only applicable for MCBCS Service.

#### 1 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 WiMAX-Session-Id which is generated by AAA after a successful initial network entry with authentication. It is delivered to the NAS in an Access-Accept packet. It is unique per CSN and is used to match all accounting records within a session.	1	1	1
Acct-Link-Count	51	This contains the number of links seen so far in this Multilink Session. It may be used to make it easier for an accounting server to know when it has all the records for a given Multilink session.	0-1	0-1	0-1
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. A PDFID belongs either to an IP-session or to an ETH-session.	0-1 [1,4]	0-1 [1,4]	0-1 [1,4]
SDFID	26/27	This value matches all packet data flows from the same service data flow.	0-1 [2,4]	0-1 [2,4]	0-1 [2,4]
Framed-IP-Address	8	The IPv4 address assigned to the MS by HCSN. 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 by HCSN. This identifies the IP Session.	0-1[3]	0-1[3]	0-1[3]
Framed-Interface-Id	96	The IPv6 interface id assigned by the Home CSN to be used for the MS. Used only for DHCPv6-based address configuration.	0-1[3]	0-1[3]	0-1[3]
Visited-Framed-IP-Address	26/79	The IPv4 address assigned to the MS by VCSN. This identifies the IP-Session.	0-1[5]	0-1[5]	0-1[5]
Visited-Framed-IPv6-Prefix	26/80	The IPv6 prefix assigned to the MS by VCSN. This identifies the IP Session.	0-1[5]	0-1[5]	0-1[5]
Visited-Framed-Interface-Id	26/81	The IPv6 interface id assigned by the visited CSN to be used for the MS. Used only for DHCPv6-based address configuration.	0-1[5]	0-1[5]	0-1[5]
MSID		ETH session identifier	0-1[3]	0-1[3]	0-1[3]
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	0-1 [1,4] [6,7]	0-1 [1,4] [6,7]	0-1 [1,4] [6,7]

Name	Type	Description	Start	Int	Stop
		scenarios.			
MCBCS-Transmission-Zone-ID	26/113	Indicates the MCBCS Transmission Zone for a given MCBCS Service.	0-1 [1,4] [6,7]	0-1 [1,4] [6,7]	0-1 [1,4] [6,7]

1 **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] Framed-IP or Framed-IPv6 or MSID SHALL be present in Accounting messages. If more than one is present then the HAAA SHALL discard the Accounting message.
- [4] SHALL NOT be included with messages coming from an HA.
- [5] If VCSN is assigning IP address either Visited Framed-IP or Visited Framed-IPv6-Prefix SHALL be present in Accounting messages. If both are present then the VAAA SHALL discard the Accounting message.
- [6] This attribute is only applicable for MCBCS Service
- [7] PDFID SHALL be used together with MCBCS Transmission Zone to uniquely identify a service flow of MBS within MCBCS Transmission Zone;

2 **5.4.1.6.3 User Identification**

Name	Type	Description	Start	Int	Stop
User-Name	1	SHOULD be the Outer-Identity of the user used during network access authentication and authorization. Note: Intermediary nodes MAY alter the decoration to accommodate deployment scenarios.	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	Set to the MAC address of the device as a 17 byte Upper Case ASCII value as defined by RFC 3580 sec 3.21 and 802-2001 in canonical order. For example "00-10-A4-23-19-C0" is Valid and 00-10-a4-23-19-c0 is not valid; and 00:10:A4:23:19:C0 is not valid.	0-1[2]	0-1[2]	0-1[2]

3 **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.

#### 1 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]
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.	0-1	0-1	0-1
HA-IP-MIP4	26/6	The IP address of the home agent.	0-1[6]	0-1[6]	0-1[6]
HA-IP-MIP6	26/7	The IP address of the home agent.	0-1[6]	0-1[6]	0-1[6]
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]
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	26/47	TBD (Geopriv has an attribute for this).	0-1[4]	0-1[4]	0-1[4]
NSP-ID	26/57	The operator ID identifying the NSP operator.	0-1[3]	0-1[3]	0-1[3]
Operator-Name	To be assigned by IETF	The WRI-Code of the VNSP and HNSP.	0-2[5]	0-2[5]	0-2[5]

#### 2 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.
- [4] Defined in IETF Geopriv.
- [5] If the VAAA included the Operator-Name in the Access-Request packet, it SHALL include it in the accounting packets. If the VAAA received the Operator-Name attribute (containing the Home operator’s WRI-Code) in an Access-Accept, it SHALL include it in the Accounting Start packet. If the attribute is included in the Accounting Start packet, it SHALL also be included in the Accounting Interim-Update (if used) and Accounting Stop packets.
- [6] If included in the AA by the AAA then SHALL be included.

#### 1 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]
Acct-Delay-Time	41	This attribute indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.	0-1	0-1	0-1

#### 2 Notes:

[1] SHALL NOT be reported by a HA.

#### 3 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 by the user. Counted after de-compression and de-fragmentation at the accounting agent.	0	0-1[2]	0-1[2]
Acct-Output-Octets	43	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-Input-Packets	47	The total number of IP packets sent by the user. Counted after de-compression and de-fragmentation at the accounting agent.	0	0-1[2]	0-1[2]
Acct-Output-Packets	48	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
Acct- Input - Gigawords	52	Incremented when attribute 42 overflows.	0	0-1[2]	0-1[2]
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[1]	0-1[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]



Name	Type	Description	Start	Int	Stop
Control-Octets-Out	26/34	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]
Acct- Input -Packets-Gigaword	26/48	Incremented when attribute 47 overflows.	0	0-1[2]	0-1[2]
Acct- Output -Packets-Gigaword	26/49	Incremented when attribute 48 overflows.	0	0-1	0-1

1 **Notes:**

- [1] SHALL NOT be reported by a HA.  
[2] SHALL Not be reported in MCBCS case

2 **5.4.1.6.7 Flow Specification**

Name	Type	Description	Start	Int	Stop
Uplink Flow-Description	26/50	IPFilter-Rule / EthFilterRule that describes an Uplink PD flow with the header fields.	0	0-n[1]	0-n[1]
Downlink Flow-Description	26/62	IPFilter-Rule / EthFilterRule that describes a Downlink PD flow with the header fields.	0	0-n[1]	0-n[1]

3 **Notes:**

- [1] The attribute SHALL not appear when Session-based accounting is performed.

For IP-CS:

- 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.

For ETH-CS:

- Ethernet specific information such as MAC address, VLAN ID and other classification rule parameters from IEEE802.16e MAY be included. When 802.1ad be used, information on S-Tags according to IEEE802.1ad MAY also be included.

If a specific field in the IPFilterRule / EthFilterRule is wild-carded, that field is not used while matching a PD flow against the IPFilterRule / EthFilterRule.

The attribute SHALL NOT be reported by a HA.

4 **5.4.1.6.8 Granted-QoS**

Name	Type	Description	Start	Int	Stop
Uplink-Granted-QoS	26/30	Uplink QoS granted to the MS.	0	0-1 [1][2]	0-1 [1][2]
Downlink-Granted-QoS	26/63	Downlink QoS granted to the MS.	0	0-1[1]	0-1[1]

**Notes:**

- [1] Attribute SHALL NOT appear when Session-based accounting is performed or from an HA.  
[2] SHALL not be reported for MCBCS Service.

**5.4.1.6.9 Flow Specification V2**

Name	Type	Description	Start	Int	Stop
Flow-Description-V2	26/83	Classifier that describes the flow. Direction is included as a part of the Classifier definition.	0	0-n [1][2]	0-n [1][2]

**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.  
SHALL NOT be reported by a HA.  
[2] SHALL not be reported for MCBCS Service.

**5.4.1.7 RADIUS Disconnect Request Message**

Disconnect Request message should be defined as per [51] 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
WiMAX-Session-Id	26/4	The NAI contained in the User-Name and the WiMAX-Session-Id forms a unique identifier of the session at the NAS.	1	0	0
WiMAX-DM-Action-Code	26/60	Carries the deregistration action code from AAA to the NAS. If the WiMAX-DM-Action-Code is not present in the RADIUS Disconnect message then the result will be to the same as if the action code 0xffff was included. The end result should be that the BS sends the RES-CMD to the MS.	0-1	0	0

RADIUS Disconnect-ACK message is sent without any additional parameters

#### 5.4.1.7.1 RADIUS Disconnect NACK Message

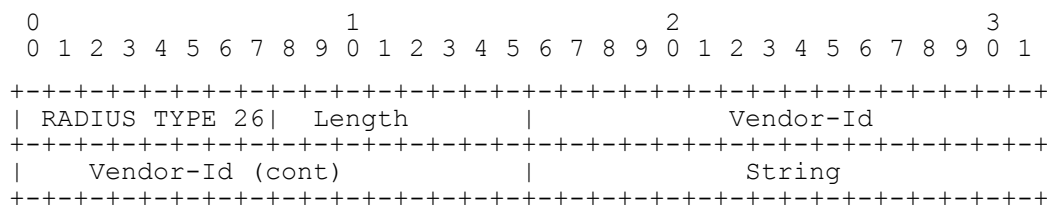
**Table 5-14 – RADIUS Disconnect NACK Message**

Attribute	ID	AR	Description	Source
Error-Cause	101	1		RFC5176

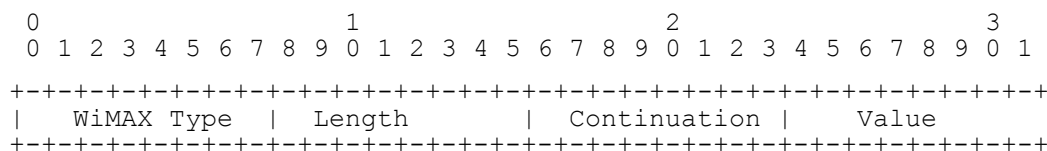
#### 5.4.2 WiMAX RADIUS VSAs Definitions

WiMAX RADIUS VSAs are transported in a RADIUS Vendor Specific Attribute.

The following describes the general format of WiMAX VSAs.



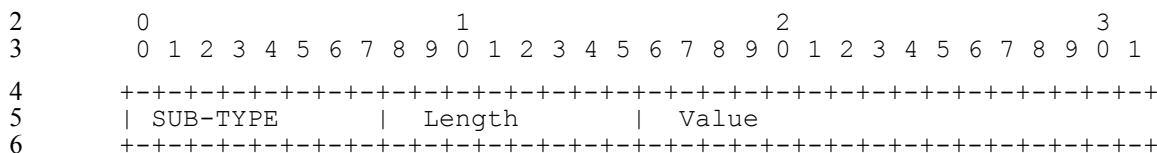
<b>Type</b>	26 for Vendor-Specific.
<b>Length</b>	Length of the entire structure which is given by: The length of the Header (=6) plus the length of the WiMAX Vendor Attribute.
<b>Vendor-Id</b>	The SMI Network Management Private Enterprise Code of the Vendor in network byte order, as defined in the "Assigned Numbers" [56]. The Vendor-Id for WiMAX is 24757.
<b>String</b>	Contains one WiMAX Vendor attribute which is formatted as specified below.



<b>WiMAX Type</b>	0 is reserved. 1-254 WiMAX Types as defined below. 255 is reserved.
<b>Length</b>	>= 3. Length of the WiMAX attribute including the WiMAX Type, length, Continuation and Value field.
<b>Continuation</b>	The Continuation Field is defined as follows: <pre> 0 0 1 2 3 4 5 6 7 +-----+   C   r   r   r   r   r   r   +-----+ </pre> 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

	<p>the next WiMAX VSA of the same WiMAX type is to be appended to this attribute.</p> <p>When the C-bit is set to zero ‘0’ this indicates that the next attribute is not a fragment of this attribute.</p> <p>A WiMAX attribute that is not being fragmented will 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.</p> <p>The r-bits are reserved for future use. They SHALL be set to zero by the sender and SHALL be ignored by the receiver.</p>
<b>Value</b>	Value of the attribute which is one of the attribute formats given below or one or more sub-TLVs.

1 A sub-TLV has the following format:



<b>WType-ID</b>	<p>0 is reserved</p> <p>1-254 WiMAX Sub-Types</p> <p>255 is reserved</p>
<b>Length:</b>	>= 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).
<b>Value</b>	Value of the attribute which is of one of the attribute formats defined below.

7 For each WiMAX VSA that consists of sub-TLVs a table summarizing the size and the presence of the TLVS in  
8 each RADIUS message is given. The table indicates whether the sub-TLV is required or not in each message and  
9 how many occurrences of the sub-TLV may appear in the message as follows:

<b>0</b>	The sub-TLV SHALL NOT appear.
<b>1</b>	The sub-TLV SHALL appear.
<b>0-1</b>	The sub-TLV MAY appear only once.
<b>0-n</b>	The sub-TLV MAY appear more than once.
<b>1-n</b>	The sub-TLV SHALL appear at least once.

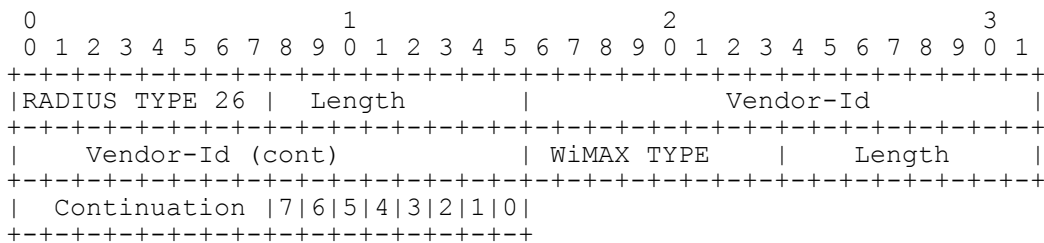
10 The abbreviations used for the column headings for these tables are:

<b>AR</b>	Access-Request or if the attribute also appears in accounting then Accounting Request.
<b>AA</b>	Access-Accept.
<b>AC</b>	Access-Challenge.
<b>R</b>	Access-Reject.

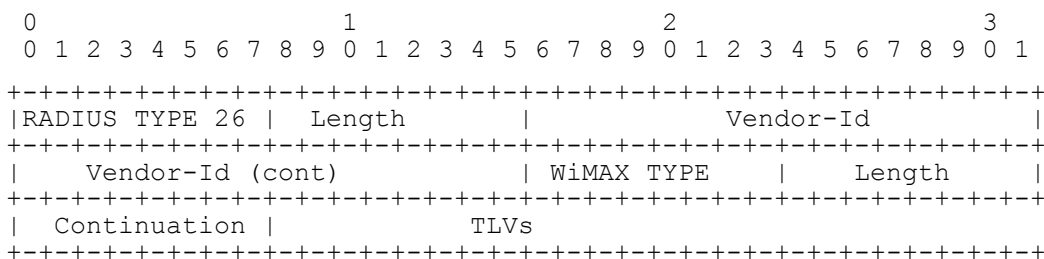
11 The following table lists the attribute formats used in describing the WiMAX VSAs.

Attribute Format	Length	Description
Unsigned-Byte	1 octets	0 to 2 <sup>8</sup> -1. Most significant bit first.
Unsigned-Short	2 octets	0 to 2 <sup>16</sup> -1. Most significant bit first.
Unsigned Integer	4 octets	0 to 2 <sup>32</sup> -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.
Bit-Map	Variable	Bit-Maps are typically 1 octet 2 octet or 4 octet in length. The most significant bit of the Bit-Map is sent first (network order) over the wire. Thus Bit-0 corresponds to the last bit received. For example for a one octet Bit Maps the bit-mask for Bit-0 is represented by the value of 0x01 (HEX). For a 2 octet Bit-Map the bit-mask for Bit-0 is represented by the value 0x0001 (HEX). See the illustration below. When a Bit is set to '1' indicates the feature is selected or supported. A Bit set to '0' indicates the feature is not selected or supported. Unless otherwise indicated unspecified bits are reserved. The sender SHALL set these bits to zero and the receiver SHALL ignore these bits.

The following diagram shows a RADIUS encoding of a 1-octet Bit-Map. The payload (value) containing the Bit-Map appears after the Continuation field. The diagram shows the positions of the bits as received by the receiver.



#### 5.4.2.1 WiMAX-Capability



<b>WType-ID</b>	1 for WiMAX-Capability Attribute
<b>Description</b>	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.
<b>Length</b>	6 + 3 + TLVs

<b>Continuation</b>	C-bit = 0
<b>Value</b>	One or more of the following sub-TLVs

1

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	WiMAX-Release	6	1	1	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
5	Packet-Flow-Descriptor-Capabilities	3	0[d]	0[d]	0	0
6	Authorized-Network-Services	6	0	1[k]	0	0
7	ASN-Network-Service-Capabilities	6	1[e][k]	0	0	0
8	VCSN-Network-Service-Capabilities	6	0-1 [f][k]	0	0	0
9	Visited-Authorized-Network-Services	3	0	0-1[g][k]	0	0
10	Authorized-Mobility-Access-Services	3	0-1[k]	0	0	0
11	ROHC-Support	3	0-1[h][k]	0-1[i][k]	0	0
12	Release-Supported	2+length of string	0-1	0	0	0
13	Version-Negotiation-Flag	2+1	0-1[j]	0	0-1	0

## 2 Notes:

- [a] The absence of this sub-TLV in an Access-Request (AR) means that the NAS or HA does not support Hot-Lining.
- [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.
- [d] The usage of this TLV is deprecated as support of Packet-Flow-Descriptor is deprecated in Rel 1.5 and Packet-Flow-Descriptor V2 SHALL only be supported.
- [e] This sub-TLV SHALL be added by ASN to indicate its supported network service capabilities.
- [f] This sub-TLV SHALL be present when MS attaches through the visited network, included by the VCSN to indicate its supported network service capabilities.
- [g] This sub-TLV SHALL be included by HCSN when MS attaches through the visited network.
- [h] The absence of this sub-TLV in an Access-Request (AR) means that the ASN does not support ROHC.
- [i] The absence of this sub-TLV in an Access-Accept (AA) message means that the HAAA does not require ROHC. The HAAA SHALL NOT send this sub-TLV to a HA. An HA SHALL silently ignore this sub-TLV.
- [j] This attribute SHALL NOT be included by the NAS.

[k] This sub-TLV SHALL not be present in RADIUS Messages between HA/LMA and AAA.

1

<b>TLV ID</b>	1 for WiMAX-Release
<b>Description</b>	In an Access-Request specifies the WiMAX release of the sender. In an Access-Accepts specifies the release selected by the HAAA for this communication. AAA Proxies SHALL NOT alter the WiMAX-Release values received in an Access-Accept. If the NAS receives a WiMAX release that it does not support it SHALL treat the Access-Accept as an Access-Reject. If the HAAA receives a release that it does not support it SHALL respond back with an Access-Reject with Error-Cause set to Invalid Request (404) as defined by RFC5176.
<b>Length</b>	2+Length of string
<b>Value</b>	A string indicating a WiMAX Release. Valid values are "1.0" or "1.5".

2

<b>TLV ID</b>	2 for Accounting-Capabilities
<b>Description</b>	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.
<b>Length</b>	2+1 octet
<b>Value</b>	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 may set All bits to 0 meaning that accounting is not required or specify one and only one of the values specified by the NAS in the Access-Request. 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. If there is a mismatch between Service Capability selection and Accounting Capability selection then the NAS SHALL treat the Access-Accept as an Access-Reject. <ul style="list-style-type: none"> <li>Bit #0 = IP/ETH-Session-based accounting. Default value for the ASN.</li> <li>Bit #1 = Flow-based accounting for IP-CS.</li> <li>Bit #2 = Flow-based accounting for ETH-CS.</li> <li>Bit #3 = R3-OC based accounting</li> <li>Bit#4 = R3-OFC based offline accounting</li> </ul> <p>Note: “R3-OC based accounting” and “R3-OFC based offline accounting” are optional flags as the requested accounting option could also be specified by pre-configuration. The Access-Accept message SHALL indicate if Diameter based or RADIUS based accounting for offline or online charging SHALL be used.</p> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

3

<b>TLV ID</b>	3 for Hotlining-Capabilities
<b>Description</b>	In an Access-Request describes the hotline capacities supported by the ASN or the HA.
<b>Length</b>	2+1 octet

<b>Value</b>	<p>In an Access-Request the NAS or HA specifies the Hot-Lining capabilities that it supports as a bit-map. If all bits are set to zero or the omission of this subTLV means that Hot-Lining is not supported.</p> <ul style="list-style-type: none"> <li>• Bit #0 = Profile-based Hot-Lining is supported (using the Hotline-Profile-ID VSA).</li> <li>• Bit #1 = Rule-based Hot-Lining is supported using NAS-Filter-Rule.</li> <li>• Bit #2 = Hot-Lining HTTP Redirection is supported.</li> <li>• Bit #3 = Rule-based Hot-Lining is supported using IP-Redirection rule.</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>
--------------	--

1

<b>TLV ID</b>	4 for Idle-Mode-Notification-Capabilities
<b>Description</b>	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.
<b>Length</b>	2+1 octet
<b>Value</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• 0x00 = Idle Mode notification is not supported or is not required.</li> <li>• 0x01 = Idle Mode notification is supported or is required.</li> </ul>

2

<b>TLV ID</b>	5 for Packet-Flow-Descriptor-Capabilities (The usage of this TLV is deprecated in this release. Only Packet-Flow-Descriptor V2 SHALL only be supported.)
<b>Description</b>	
<b>Length</b>	
<b>Value</b>	

3

<b>TLV ID</b>	6 for Authorized-Network-Services
<b>Description</b>	<p>This TLV is included in a RADIUS Access-Accept packet to the NAS and indicates which Network Service Capabilities with anchoring in the HCSN the ASN is authorized to provide to the MS.</p> <p>Note: A NAS that supports this attribute MAY treat the information as a hint as to the mobility capabilities of the MS rather than an authorization for the use of mobility services.</p>
<b>Length</b>	2+4 octet
<b>Value</b>	<p>4 octet Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 – CMIP4</li> <li>• Bit #1 – PMIP4</li> <li>• Bit #2 – Simple IPv4</li> <li>• Bit #3 – CMIP6</li> <li>• Bit #4 – PMIP6</li> <li>• Bit #5 – Simple IPv6</li> </ul>



	<ul style="list-style-type: none"> <li>• Bit #6 – Simple ETH Service</li> <li>• Bit #7 – MIP based ETH Service</li> <li>• Bit #8 – L2 DHCP Relay<sup>[a]</sup></li> </ul> <p>The rest of the bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>
--	---

[a] L2 DHCP Relay can be selected with either Simple Ethernet Service or MIP based Ethernet Service.

<b>TLV ID</b>	7 for ASN-Network-Service-Capabilities
<b>Description</b>	This TLV is included in a RADIUS Access-Request packet to the RADIUS server and indicates related Network Service Capabilities ASN is willing to support
<b>Length</b>	2+4 octet
<b>Value</b>	<p>4 octet Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 – DHCPv4 Relay</li> <li>• Bit #1 – DHCPv6 Relay</li> <li>• Bit #2 – DHCPv4 Proxy</li> <li>• Bit #3 – DHCPv6 Proxy</li> <li>• Bit #4 – FA</li> <li>• Bit #5 – PMIP Client</li> <li>• Bit #6 – AR with IPv4 Transport<sup>30</sup></li> <li>• Bit #7 – AR with IPv6 Transport<sup>31</sup></li> <li>• Bit #8 – L2FW</li> <li>• Bit #9 – ETH Service FA</li> <li>• Bit #10 – L2 DHCP Relay</li> <li>• Bit #11 – MAG</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

<b>TLV ID</b>	8 for VCSN-Network-Service-Capabilities
<b>Description</b>	This TLV is included in a RADIUS Access-Request packet to the RADIUS server and indicates VCSN related Network Service Capabilities
<b>Length</b>	2+4 octet
<b>Value</b>	<p>4 octet Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 – DHCPv4 Server</li> <li>• Bit #1 – DHCPv6 Server</li> <li>• Bit #2 – HAv4</li> <li>• Bit #3 – HAv6</li> <li>• Bit #4 – eCB</li> <li>• Bit #5 – ETH HA</li> </ul>

<sup>30</sup> AR with IPv4 transport indicates the support of Simple IP service using IPv4 transport

<sup>31</sup> AR with IPv6 transport indicates the support of Simple IP service using IPv6 transport

	<ul style="list-style-type: none"> <li>• Bit #6 – LMA</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>
--	--

1

<b>TLV ID</b>	9 for Visited-Authorized-Network-Services
<b>Description</b>	This TLV is included in a RADIUS Access-Accept packet to the NAS and indicates which Network Services (ETH or IP) are authorized to be anchored in the VCSN.
<b>Length</b>	2+4 octet
<b>Value</b>	<p>4 octet Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 – CMIP4</li> <li>• Bit #1 – PMIP4</li> <li>• Bit #2 – Simple IPv4</li> <li>• Bit #3 – CMIP6</li> <li>• Bit #4 – PMIP6</li> <li>• Bit #5 – Simple IPv6</li> <li>• Bit #6 – Simple ETH Service</li> <li>• Bit #7 – MIP based ETH Service</li> <li>• Bit #8 – L2 DHCP Relay<sup>[a]</sup></li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

2 [a] L2 DHCP Relay can be selected with either Simple ETH Service or MIP based ETH Service

3

<b>TLV ID</b>	10 for Mobility-Access-Capabilities
<b>Description</b>	In an Access-Request describes mobility access supported by the ASN.
<b>Length</b>	2+1 octet
<b>Value</b>	<p>In an Access-Request the NAS indicates its mobility access capabilities that it supports as a bit-map. A value of zero or the omission of this subTLV means that Fixed and Nomadic access are not supported.</p> <ul style="list-style-type: none"> <li>• Bit#0 = Fixed/Nomadic access is not supported. Only Mobility.</li> <li>• Bit#1 = Fixed/Nomadic access is supported alongside Mobility.</li> <li>• Bit#2 = Only Fixed/Nomadic access is supported. No Mobility.</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

4

<b>TLV ID</b>	11 for ROHC-Support
<b>Description</b>	In an Access-Request or Accept-Accept describes the ROHC capability supported by the ASN or required by the CSN. Omission of this sub TLV means that ROHC capability is not supported or required.
<b>Length</b>	2+1 octet
<b>Value</b>	In an Access-Request the NAS (ASN) specifies if ROHC capability is supported at the ASN. In Access-Accept the HAAA specifies if ROHC capability is required. A value of zero or the omission of this subTLV means that ROHC is not supported.

	<ul style="list-style-type: none"> <li>• Bit #0 = ROHC capability is supported or is required.</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>
--	---

1

<b>TLV ID</b>	12 for Release-Supported
<b>Description</b>	This TLV is included by the NAS in a AAA request message to the HAAA and indicates which WiMAX versions are supported by the NAS or by the VAAA (if the VAAA is participating in the version negotiation). The attribute SHALL NOT be sent in a AAA Answer message.
<b>Length</b>	2+length of string
<b>Value</b>	String of supported releases separated by commas ','. The list is ordered from the lowest version to the highest version supported.

2

<b>TLV ID</b>	13 for Version-Negotiation-Flag
<b>Description</b>	<p>This TLV SHALL be included in a AAA request message by the VAAA to indicate that the VAAA is agreeing with the proposed version by the NAS or if it is proposing its own version in the WiMAX-Release TLV.</p> <p>The attribute MAY be included in the AAA answer message set to the value of three(3) by the HAAA to indicate to the VAAA and NAS that the Challenge message is announcing the negotiated version only. The NAS will have to re-issue the request message encode with the version proposed in the WiMAX-Release TLV of the WiMAX-Capability attribute.</p>
<b>Length</b>	2+1 octet
<b>Value</b>	<p>One octet enumeration with the following value:</p> <ul style="list-style-type: none"> <li>[1] Indicating that the VAAA has agreed to the version proposed by the NAS. This implies that the Access-Request is coded in accordance with the indicated WiMAX-Release.</li> <li>[2] Indicates that the VAAA has modified the version proposed by the NAS. This means that the HAAA SHALL use this exchange for version negotiation only.</li> <li>[3] Set by the HAAA to indicate that the Access-Challenge is for version negotiation only.</li> </ul> <p>All other values are reserved.</p>

3

#### 5.4.2.2 Void

#### 5.4.2.3 GMT-Time-Zone-Offset

```

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 | Time-Zone-offset
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+---+---+---+---+---+

```

<b>WType-ID</b>	3 for GMT-Timezone-offset
<b>Description</b>	The current offset in seconds of the local time at the NAS with respect to GMT time.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	4 Octet-String interpreted as a Signed Integer (Most significant bit first) indicating a timeoffset in seconds.

#### 5.4.2.4 WiMAX-Session-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 | WiMAX-Session-Id
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	4 for WiMAX-Session-Id
<b>Description</b>	<p>A unique per realm identifier assigned to the WiMAX session by the hAAA during network entry.</p> <p>The same value is included in all subsequent AAA transactions packets for that WiMAX session.</p> <p>A WiMAX session is established when the MS performs a successful initial network entry. The WiMAX session is terminated when network exit procedures are performed.</p>
<b>Length</b>	6 + 3 + Length of ID
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet String. The value of the WiMAX-Session-Id.

1

2  
3  
4  
5  
6  
7  
8  
9  
10

<b>WType-ID</b>	5 for MSK
<b>Description</b>	The Master Session Key determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication.
<b>Length</b>	6 + 3 + 2(SALT) + length of the String containing the encrypted MSK.
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2 octet SALT (see [39]) and String containing the encrypted MSK formulated as per [39].

## 11

12  
13  
14  
15  
16  
17  
18  
19  
20

<b>WType-ID</b>	6 for hHA-IP-MIP4
<b>Description</b>	The IPv4 address of the h-HA for MIP4v4.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv4 address (most significant bit first).

## 21

22  
23  
24  
25  
26  
27  
28  
29  
30

<b>WType-ID</b>	7 for hHA-IP-MIPv6
<b>Description</b>	The IPv6 address of the h-HA used for MIPv6.
<b>Length</b>	6 + 3 + 16
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv6 address (most significant bit first).

#### 5.4.2.8 hDHCPv4-Server

```

1
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          | DHCP-Server IPv4
10     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	8 for hDHCPv4-Server
<b>Description</b>	The IPv4 address of the home DHCP-Server to use for IPv4 address allocation by the ASN.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv4 address (most significant bit first).

#### 5.4.2.9 hDHCPv6-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 IPv6
20     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	9 for hDHCPv6-Server
<b>Description</b>	The IPv6 address of the home DHCP-Server to use for IPv6 allocation by the ASN.
<b>Length</b>	6 + 3 + 16
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv6 address (most significant bit first).

#### 5.4.2.10 MN-hHA-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          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	10 for MN-hHA-MIP4-KEY
<b>Description</b>	The MN-hHA-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 Home HA to validate the MN-HA-AE (CMIP4) and to compute the MN-HA-AE for of the CMIP4 Registration Response and the SPI.
<b>Length</b>	6 + 3 +2(SALT)+ Length of the encrypted MN-hHA-MIP4-KEY
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2 octet SALT (see [39]) and String containing the encrypted MN-hHA-MIP4-KEY formulated as per [39].

#### 5.4.2.11 MN-hHA-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              |                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               |                               |                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	11 MN-hHA-MIP4-SPI
<b>Description</b>	The SPI associated with the MN-HA-MIP4-KEY.
<b>Length</b>	6+3+4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit Integer. In an Access-Accept sent from the home AAA to the ASN the value is set to SPI-PMIP4.

#### 5.4.2.12 MN-hHA-MIP6-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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	12 for MN-hHA-MIP6-KEY
<b>Description</b>	The MN-hHA-MIP6-KEY sent by the RADIUS Server to the HA used for CMIP6. It is sent to the HA to validate AUTH and to compute the AUTH for MIP6 Binding Answer.
<b>Length</b>	6 + 3 + 2(SALT)+ Length of the encrypted MN-hHA-MIP6-KEY
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2 octet SALT (see [39]) and String containing the encrypted MN-hHA-MIP6-KEY formulated as per [39].

#### 5.4.2.13 MN-hHA-MIP6-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              |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	13 MN-hHA-MIP6-SPI
<b>Description</b>	The SPI associated with the MN-hHA-MIP6-KEY/
<b>Length</b>	6 +3+4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit Integer.



#### 5.4.2.14 FA-RK-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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	14 for FA-RK-KEY
<b>Description</b>	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.
<b>Length</b>	6 + 3 + 2(SALT) + length of the String containing the encrypted FA-RK-KEY.
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2-octet SALT (see [39]) and String containing the encrypted FA-RK formulated as per [39].

#### 5.4.2.15 hHA-RK-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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	15 for hHA-RK-KEY
<b>Description</b>	The hHA-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.
<b>Length</b>	6 + 3 + 2(SALT) + length of the String containing the encrypted hHA-RK-KEY.
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2-octet SALT (see [39]) and String containing the encrypted HA-RK formulated as per [39].



<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv4 or IPv6 address (most significant bit first).

#### 5.4.2.19 RRQ-MN-HA-KEY

```

0
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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	19 for RRQ-MN-HA-KEY
<b>Description</b>	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.
<b>Length</b>	6 + 3 +2(SALT)+ Length of the encrypted RRQ-MN-HA-KEY
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2-octet SALT (see [39]) and String containing the encrypted RRQ-MN-HA-KEY formulated as per [39].

#### 5.4.2.20 Time-Of-Day-Time

```

0
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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	20 for Time-Of-Day-Time
<b>Description</b>	The attribute identifies the time in a day at which a tariff switch occurs for volume-based billing and duration-based billing.
<b>Length</b>	6 + 3 + Length of Sub TLVs
<b>Continuation</b>	C-bit = 0
<b>Value</b>	The following sub-TLVs

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	Hour	3	0	1	0	0

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
2	Minute	3	0	1	0	0
3	UTC Offset	6	0	1	0	0

<b>TLV ID</b>	1 for Hour
<b>Description</b>	Specifies the hour of the day in 24-hour format for the tariff change.
<b>Length</b>	2+1 octet
<b>Value</b>	0-23

<b>TLV ID</b>	2 for Minute
<b>Description</b>	Specifies the minute of the hour for the tariff change.
<b>Length</b>	2+1 octet
<b>Value</b>	0-59

<b>TLV ID</b>	3 for UTC Offset
<b>Description</b>	Specifies the time zone offset from UTC for the tariff change in seconds.
<b>Length</b>	2+4 octets
<b>Value</b>	

#### 5.4.2.21 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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+---+---+---+---+---+---+

```

<b>WType-ID</b>	21 for Session-Continue
<b>Description</b>	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.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	If the value is set to 1 session continue is true. If the value is set to 0 session continue is false.

#### 5.4.2.22 Beginning-of-Session

```

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 | Beginning of Session Flag
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	22 for Beginning-of-Session
<b>Description</b>	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.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	If the value is set to 1 Beginning-of-Session is true. If the value is set to 0 Beginning-of-Session is false.

#### 5.4.2.23 Network-Technology

```

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 | Network-Technology Enumeration
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	23 for Network-Technology
<b>Description</b>	This attribute indicates which type of WiMAX session is being used.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer. The enumeration is defined as follows: <ul style="list-style-type: none"> <li>• 0 = Simple IPv4</li> <li>• 1 = Simple IPv6</li> <li>• 2 = PMIP4</li> <li>• 3 = CMIP4</li> <li>• 4 = CMIP6</li> <li>• 5 = Ethernet-CS</li> <li>• 6 = Simple ETH</li> <li>• 7 = MIP based ETH</li> <li>• 8 = PMIP6</li> <li>• 9 - 2<sup>32</sup>-1 = Reserved</li> </ul>

1

2

3

## 11

12

13

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	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																															

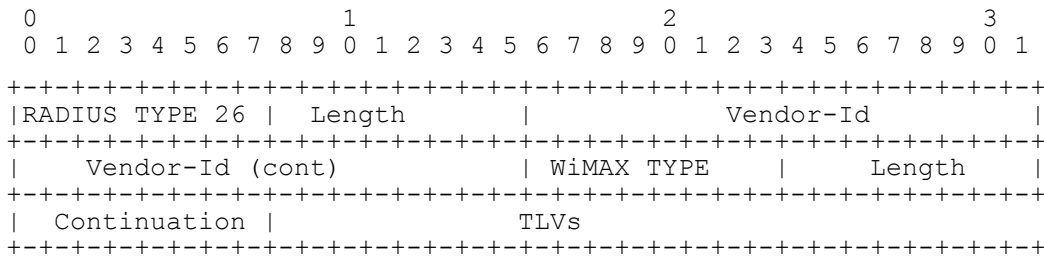
#### 5.4.2.27 SDFID

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	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																															

#### 5.4.2.28 Packet-Flow Descriptor (This Attribute is deprecated in this release)<sup>32</sup>

WiMAX FORUM PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

#### 5.4.2.29 QoS-Descriptor



<b>Type-ID</b>	29 for QoS-Descriptor
<b>Description</b>	This attribute describes over the air QoS parameters that are associated with a flow. The QoS-Descriptor is only valid for the actual RADIUS transaction.  QoS-Descriptor is used for describing both PPSFs and dynamic SFs, and Dynamic reservation flag in Activation Trigger TLV makes the distinction between the two. For dynamic SFs, QoS-Descriptor represents the information that can be used in an implementation specific manner in authorization check.
<b>Length</b>	6 + 3 + TLVs
<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	The sub-types are described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR	COA	COA-ACK	COA-NAK
1	QoS ID	3	0	1	0	0	1	0	0
2	Global Service Class Name	2+6	0	0-1	0	0	0-1	0	0
3	Service Class Name	2+Length	0	0-1	0	0	0-1	0	0
4	Schedule Type	3	0	1	0	0	1	0	0
5	Traffic Priority	3	0	0-1[a][b]	0	0	0-1[a][b]	0	0
6	Maximum Sustained Traffic Rate	6	0	0-1[a]			0-1[a]		
7	Minimum Reserved Traffic Rate	6	0	0-1[a]	0	0	0-1[a]	0	0
8	Maximum Traffic Burst	6	0	0-1[a]	0	0	0-1[a]	0	0
9	Tolerated Jitter	6	0	0-1[a]	0	0	0-1[a]	0	0
10	Maximum Latency	6	0	0-1[a]	0	0	0-1[a]	0	0
11	Reduced Resources Code	3	0	0-1[a][d]	0	0	0-1[a][d]	0	0
12	Media Flow Type	2+1	0	0-1[a]	0	0	0-1[a]	0	0
13	Unsolicited Grant Interval	4	0	0-1[a]	0	0	0-1[a]	0	0
14	SDU Size	2+1	0	0-1[a]	0	0	0-1[a]	0	0
15	Unsolicited Polling Interval	4	0	0-1[a]	0	0	0-1[a]	0	0



TLV ID	TLV Name	Length Octets	AR	AA	AC	AR	COA	COA-ACK	COA-NAK
16	Media Flow Description in SDP Format	2 + Length	0	0-1	0	0	0-1	0	0
17	Transmission policy	1	0	0-1[c]	0	0	0-1[c]	0	0
18	DSCP	2+1	0	0-1	0	0	0-1	0	0

1 **Notes:**

- [a] The inclusion of these attributes is as per the value of the Schedule-Type in accordance to Table 5-15.
- [b] If omitted the traffic priority is assumed to be 0.
- [c] If omitted the Transmission policy is assumed to be 0. If included, the ASN MAY ignore it.
- [d] This attribute is not applicable for MCBSC Service.

2 **Table 5-15 – 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]	1	0-1[b]	0-1[b]
7	Minimum reserved traffic rate	0	1	0-1[e]	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
17	Transmission policy	0-1[f]	0-1[f]	0-1[f]	0-1[f]	0-1[f]

3 **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.
- [e] If present, it SHALL have the same value as the Maximum Sustained Traffic Rate parameter.
- [f] If omitted the Transmission policy is assumed to be 0. If included the ASN MAY ignore it.

4

<b>TLV ID</b>	1 for QoS ID
---------------	--------------

<b>Description</b>	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).
<b>Length</b>	2+1
<b>Value</b>	Unsigned Octet representing an ID.

1

<b>TLV ID</b>	2 for Global Service Class Name
<b>Description</b>	This parameter represents the Global Service Class Name as defined in IEEE802.16e.
<b>Length</b>	2+6
<b>Value</b>	String of length 6 octet containing the name of the global service class name. Values are defined in IEEE802.16e.

2

<b>TLV ID</b>	3 for Service Class Name
<b>Description</b>	This parameter represents the Service Class Name as defined in IEEE802.16e.
<b>Length</b>	2+Length of Service Class String (>=1)
<b>Value</b>	String containing the name of the service class name. Values are defined in IEEE802.16e.

3

<b>TLV ID</b>	4 for Schedule Type
<b>Description</b>	The parameter specifies the Uplink Granted Scheduling Type as defined in IEEE802.16e.
<b>Length</b>	2+1
<b>Value</b>	Octet enumeration with the following values defined: <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = Reserved</li> <li>• 2 = Best Effort</li> <li>• 3 = nrtPS</li> <li>• 4 = rtPS</li> <li>• 5 = Extended rtPS</li> <li>• 6 = UGS</li> <li>• 7 – 255 = Reserved</li> </ul>

4

<b>TLV ID</b>	5 for Traffic Priority
<b>Description</b>	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.
<b>Length</b>	2+1
<b>Value</b>	0 to 7 – Higher numbers indicate higher priority. Default 0.

5

<b>TLV ID</b>	6 for Maximum Sustained Traffic Rate
<b>Description</b>	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.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer specifying a rate in bits per second.

1

<b>TLV ID</b>	7 for Minimum Reserved Traffic Rate
<b>Description</b>	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.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer specifying the rate in bytes.

2

<b>TLV ID</b>	8 for Maximum Traffic Burst
<b>Description</b>	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.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer specifying the burst size in bytes per second as defined by IEEE802.16e.

3

<b>TLV ID</b>	9 for Tolerated Jitter
<b>Description</b>	Represents the Tolerated Jitter as defined in IEEE802.16e.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer representing the maximum delay variation (jitter) (in milliseconds).

4

<b>TLV ID</b>	10 for Maximum Latency
<b>Description</b>	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.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer specifying a maximum latency in units of milliseconds.

1

<b>TLV ID</b>	11 for Reduced Resources Code
<b>Description</b>	This code indicates that the requesting entity will accept reduced resources if the requested resources are not available.
<b>Length</b>	2+1
<b>Value</b>	Unsigned Octet: value of 0 is not allowed, value of 1 allowed. Other values are reserved.

2

<b>TLV ID</b>	12 for Media Flow Type
<b>Description</b>	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
<b>Length</b>	2+1
<b>Value</b>	<p>The first octet of the string represents an enumeration with the following values:</p> <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = Voice over IP</li> <li>• 2 = Robust Browser</li> <li>• 3 = Secure Browser/ VPN</li> <li>• 4 = Streaming video on demand</li> <li>• 5 = Streaming live TV</li> <li>• 6 = Music and Photo Download</li> <li>• 7 = Multi-player gaming</li> <li>• 8 = Location-based services</li> <li>• 9 = Text and Audio Books with Graphics</li> <li>• 10 = Video Conversation</li> <li>• 11 = Message</li> <li>• 12 = Control</li> <li>• 13 = Data</li> <li>• 14 – 255 = Reserved</li> </ul>

3

<b>TLV ID:</b>	13 for Unsolicited Grant Interval
<b>Description:</b>	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).
<b>Length:</b>	2+2
<b>Value:</b>	Unsigned Short measuring time in milliseconds.

4

<b>TLV ID</b>	14 for SDU Size
---------------	-----------------

<b>Description</b>	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.
<b>Length</b>	2+1
<b>Value</b>	8-bit unsigned integer. Default = 49.

1

<b>TLV ID</b>	15 for Unsolicited Polling Interval
<b>Description</b>	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
<b>Length</b>	2+2
<b>Value</b>	16-bit unsigned integer representing the polling interval (in milliseconds).

2

<b>TLV ID</b>	16 for Media Flow Description in SDP format
<b>Description</b>	This is a variable length string having SDP information. The <SDP string> is encoded as specified in IETF RFC 2327.
<b>Length</b>	2+String
<b>Value</b>	<SDP string> is encoded as specified in IETF RFC 2327.

3

<b>TLV ID</b>	17 for Transmission Policy
<b>Description</b>	The parameter indicates the transmission policy of a service flow.
<b>Length</b>	2+1
<b>Value</b>	<p>Octet enumeration with the following values defined:</p> <ul style="list-style-type: none"> <li>• Bit #0 – Service flow SHALL NOT use broadcast bandwidth request opportunities. (Uplink only)</li> <li>• Bit #1 –Service flow SHALL NOT use multicast bandwidth request opportunities. (Uplink only).</li> <li>• Bit #2 – The service flow SHALL NOT piggyback requests with data. (Uplink only)</li> <li>• Bit #3 – The service flow SHALL NOT fragment data.</li> <li>• Bit #4 – The service flow SHALL NOT suppress payload headers (CS parameter).</li> <li>• Bit #5 – The service flow SHALL NOT pack multiple SDUs (or fragments) into single MAC PDUs.</li> <li>• Bit #6 – The service flow SHALL NOT include CRC in the MAC PDU.</li> <li>• Bit #7 – The service flow SHALL NOT compress payload headers using ROHC.</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p> <p>Note: The bit#7 is reserved prior to NWG release 1.5</p>

4

<b>TLV ID</b>	18 for DSCP
<b>Description</b>	Differentiated services code point as defined in RFC 2474 [29]. <u>Used to mark the bearer IP</u>

2

## 3

11

13

## 14

25

Page - 818  
WiMAX FORUM PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer representing packets count.

#### 5.4.2.32 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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+---+---+---+---+---+---+

```

<b>WType-ID</b>	32 for Control-Octets-In
<b>Description</b>	Octet counts for incoming Mobile IPv4, DHCP, ICMP messages etc.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer representing octets.

#### 5.4.2.33 Control-Packets-Out

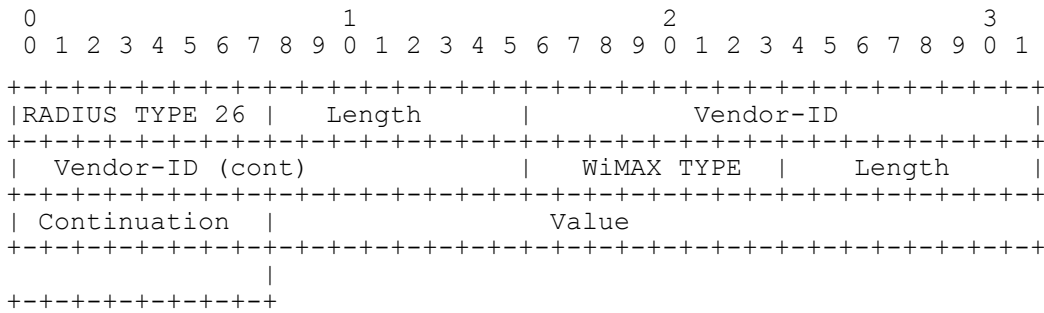
```

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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+---+---+---+---+---+---+

```

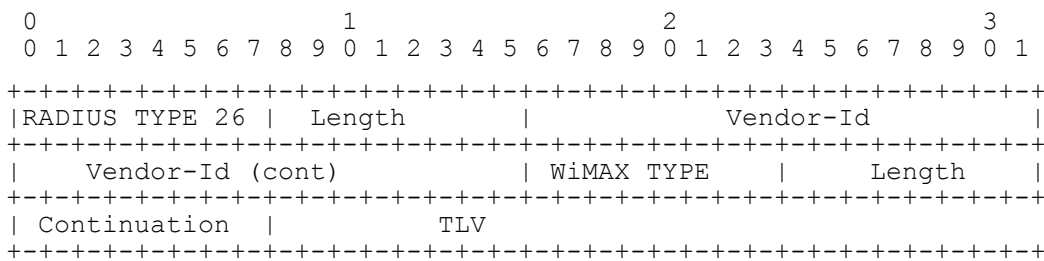
<b>WType-ID</b>	33 for Control-Packets-Out
<b>Description</b>	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer representing packets count.

#### 5.4.2.34 Control-Octets-Out



<b>WType-ID</b>	34 for Control-Octets-Out
<b>Description</b>	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer representing an octet count.

#### 5.4.2.35 PPAC



<b>WType-ID</b>	35 for PPAC
<b>Description</b>	The PrepaidAccountingCapability (PPAC) attribute is sent in the Access-Request packet by a prepaid capable NAS and is used to describe the prepaid capabilities of the NAS.
<b>Length</b>	6 + 3 + TLVs
<b>Continuation</b>	C-bit = 0.
<b>Value</b>	The sub-types described below.

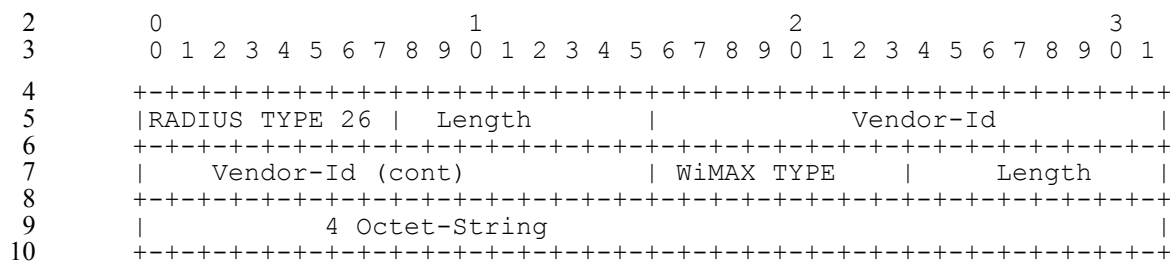
TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	AvailableInClient (AiC)	2+4	1	0	0	0

<b>TLV ID</b>	1 for AvailableInClient (AiC)
<b>Description</b>	The optional AvailableInClient Subtype, generated by the PPC, indicates the metering capabilities of the NAS and SHALL be bit-map encoded. The possible values are as follows.
<b>Length</b>	2+4



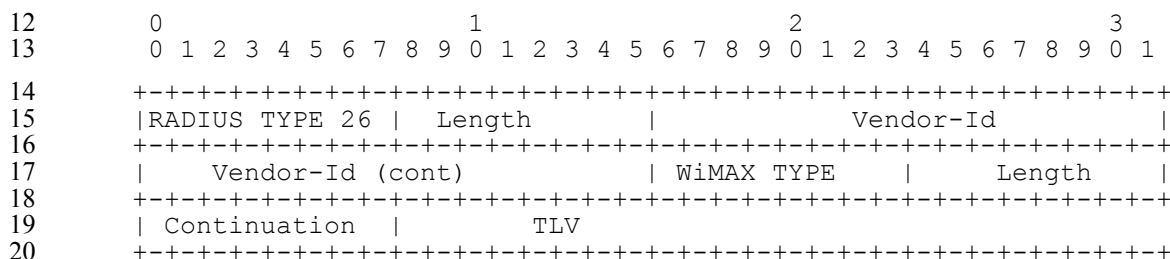
<b>Value</b>	<p>4 Octet String interpreted as a bit map with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 - Volume metering supported</li> <li>• Bit #1 - Duration metering supported</li> <li>• Bit #2 - Resource metering supported</li> <li>• Bit #3 - Pools supported</li> <li>• Bit #4 - Rating groups supported</li> <li>• Bit #5 - Multi-Services supported</li> <li>• Bit #6 - Tariff Switch supported</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>
--------------	---

#### 5.4.2.36 Session Termination Capability



<b>WType-ID</b>	36 for Session Termination Capability
<b>Description</b>	This attribute is included in a RADIUS Access-Request packet to the RADIUS server and indicates whether or not the NAS supports Dynamic Authorization.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	<p>4 octet Bit Map with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 - Dynamic Authorization Extensions ([51]) is supported</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

#### 5.4.2.37 PPAQ Attribute



<b>WType-ID</b>	37 for PPAQ
<b>Description</b>	One or more PPAQ attributes are sent in an Access-Request, Authorize- Only Access-Request and Access-Accept packet. In an Access-Request packet, the PPAQ attribute is used to facilitate One-Time charging transactions. In Authorize-Only Access-Request packets 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 packet 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). For IP Session based Accounting, there SHALL be just one PPAQ per IP-Session.
<b>Length</b>	6 + 3 + TLVs
<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	The sub-types described below.

1

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	Volume-Quota	2+(8 or 12)	0-1[a][g]	0-1[a][k][n]	0	0
3	Volume-Threshold	2+(8 or 12)	0	0-1[a][m][n]	0	0
4	Duration-Quota	2+4	0-1[b][g]	0-1[b][k][n]	0	0
5	Duration-Threshold	2+4	0	0-1[b][m][n]		
6	Resource-Quota	2+(8 or 12)	0-1[c][g]	0-1[c][k][n]	0	0
7	Resource-Threshold	2+(8 or 12)	0	0-1[c][m][n]	0	0
8	Update-Reason	2+1	0-1[d][g]	0	0	0
9	Prepaid-Server	2+Length	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+(8 or 12)	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
17	Cost-Information	2+16+length	0	0-1[n]	0	0

2 **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 Volume-Quota, Duration-Quota or Resource-Quota 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 Quota-Identifier, 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.

1

<b>TLV ID</b>	1 for Quota-Identifier
<b>Description</b>	It is generated by the PPS together with the allocation of new quota. The online quota update RADIUS Access-Request packet that is sent from the PPC to the PPS includes a previously received QuotaIdentifier AVP.
<b>Length</b>	2+Length of Quota-Identifier (Quota-Identifier not to exceed 4 octets)
<b>Value</b>	Octet String. The Quota-Identifier value (most significant bit first).

2

<b>TLV ID</b>	2 for Volume-Quota
<b>Description</b>	The length of this AVP is 10 or 14 octets. In a RADIUS Access-Accept packet (PPS to PPC direction), it indicates the volume (in octets) excluding control data (as defined in section 5.4.2.31) allocated for the session by the PPS. In an RADIUS Authorize-Only Access-Request packet (PPC to PPS direction), it indicates the total used volume (in octets) for both inbound and outbound traffic. The attribute consists of a Value-Digits field and optionally an Exponent field (as indicated in the length field).
<b>Length</b>	2+(8 or 12)
<b>Value</b>	<ul style="list-style-type: none"> <li>• 8 octets = Value-Digits field is an Unsigned64 value which contains the significant digits of the number. If decimal values are needed to present the units, the scaling MUST be indicated with the related Exponent field.</li> <li>• 4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field.</li> </ul>

3

<b>TLV ID:</b>	3 for Volume-Threshold
<b>Description:</b>	This AVP is optionally present if Volume-Quota is present in a RADIUS Access-Accept packet (PPS to PPC 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 Volume Quota. The attribute consists of a Value-Digits field and optionally an Exponent field (as indicated by the length field).
<b>Length:</b>	2+(8 or 12)

<b>Value:</b>	<ul style="list-style-type: none"> <li>8 octets = Value-Digits field is an Unsigned64 value which contains the significant digits of the number. If decimal values are needed to present the units, the scaling MUST be indicated with the related Exponent field.</li> <li>4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field.</li> </ul>
---------------	--

1

<b>TLV ID</b>	4 for Duration-Quota
<b>Description</b>	This optional AVP is only present if duration-based charging is used. In RADIUS Access-Accept packet (PPS to PPC 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-Request message (PPC to PPS direction), it may indicate the total duration (in seconds) since the start of the accounting session related to the QuotaID of the PPAQ in which it occurs.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer representing seconds.

2

<b>TLV ID</b>	5 for Duration-Threshold
<b>Description</b>	This AVP is optionally present if Duration-Quota is present in a RADIUS Access-Accept packet (PPS to PPC 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 Duration-Quota.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer representing seconds.

3

<b>TLV ID</b>	6 for Resource-Quota
<b>Description</b>	This optional AVP is only present if resource-based or one-time charging is used. In the RADIUS Access-Accept packet (PPS to PPC direction) it indicates the resources allocated for the session by the PPS. In RADIUS Authorize-Only Access-Request packet (PPC 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. The attribute consists of a Value-Digits field and optionally an Exponent field (as indicated by the length field).
<b>Length</b>	2+(8 or 12)
<b>Value</b>	<ul style="list-style-type: none"> <li>8 octets = Value-Digits field is an Unsigned64 value which contains the significant digits of the number. If decimal values are needed to present the units, the scaling MUST be indicated with the related Exponent field.</li> <li>4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field.</li> </ul>

4

<b>TLV ID</b>	7 for Resource-Threshold
<b>Description</b>	The semantics of this AVP follows those of the Volume-Threshold and Duration-Threshold AVPs. It consists of a Value-Digits field and optionally an Exponent field.
<b>Length</b>	2+(8 or 12)
<b>Value</b>	<ul style="list-style-type: none"> <li>8 octets = Value-Digits field is an Unsigned64 value which contains the significant</li> </ul>

	<p>digits of the number. If decimal values are needed to present the units, the scaling MUST be indicated with the related Exponent field.</p> <ul style="list-style-type: none"> <li>4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field.</li> </ul>
--	--

1

<b>TLV ID</b>	8 for Update-Reason
<b>Description</b>	This AVP SHALL be present in the Authorize-Only RADIUS Access-Request packet (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 packet.
<b>Length</b>	2+1
<b>Value</b>	<p>Octet enumeration with the following values:</p> <ul style="list-style-type: none"> <li>0 = Reserved</li> <li>1 = Pre-initialization</li> <li>2 = Initial-Request</li> <li>3 = Threshold Reached</li> <li>4 = Quota Reached</li> <li>5 = TITSU Approaching</li> <li>6 = Remote Forced Disconnect</li> <li>7 = Client Service Termination</li> <li>8 = “Access Service” Terminated</li> <li>9 = Service not established</li> <li>10 = One-time Charging</li> </ul>

2

<b>TLV ID</b>	9 for Prepaid-Server
<b>Description</b>	<p>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.</p> <p>If present in the incoming RADIUS Access-Accept packet, the PPC SHALL send this attribute back without modifying it in the subsequent RADIUS Access-Request packet, except for the first one. If multiple values are present, the PPC SHALL not change their order.</p>
<b>Length</b>	2 + (4 (IPv4) or 16 (IPv6))
<b>Value</b>	The value of this AVP is encoded as an IPv4 address or an IPv6 address.

3

<b>TLV ID</b>	10 for Service-ID
<b>Description</b>	<p>This value is a string that uniquely describes the service instance to which prepaid metering should be applied.</p> <p>A Service-Id SHALL be one of: (a) IP 5-tuple (source address, source port, destination address, destination port, protocol) for IP Service or MSID for Ethernet Service, (b) PDFID or (c) SDFID or (d) IP address. 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,</p>

	then the PPAQ refers to the Access Service (ISF). For IP Session based accounting only one Service-ID encoded as below SHALL be included.
<b>Length</b>	2+ Length of Service-ID
<b>Value</b>	<p>The value field of this AVP is encoded as a UTF8 string as follows:</p> <p>To encode an IP-Tuple for flow based accounting the syntax used in the IPFilterRule of RFC3588 is used as follows:</p> <p>“iptuple=” dir proto “from” src “to” dst</p> <p>dir, proto, src and dst are as per RFC3588 filter rule and include the keywords “assigned” when the IP address of the MS is not known at time of issue. To encode one or more PDFID use the following:</p> <p>“pdfid=”pdfid1 (encoding if there is one PDFID) OR</p> <p>“pdfid= “pdfid1,pdfid2,... (encoding if there are two or more PDFIDs)</p> <p>where: pdfid is the ascii hex representation of the PDFID as in (0xfada)</p> <p>To encode one or more SDFIDs:</p> <p>“sdfid=”sdfid1 (encoding if there is one SDFID) OR</p> <p>“sdfid=” sdfid1,sdfid2,... (encoding if there are two or more SDFIDs)</p> <p>where: sdfid is the ascii hex representation of the SDFID as in (0xfada)</p> <p>For IP session based accounting :</p> <p>IP Address is encoded as ASCII hex using IPFilterRule format of 3588.</p> <p>“assigned” if IP address is unknown or ASCII version of IP address i.e. “1.2.3.4”.</p>

1

<b>TLV ID</b>	11 for Rating-Group-ID
<b>Description</b>	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.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer representing the value of the Rating Group ID.

2

<b>TLV ID</b>	12 for Termination-Action
<b>Description</b>	This AVP describes action to take when the PPS does not grant additional quota.
<b>Length</b>	2+1
<b>Value</b>	<p>Octet Enumeration with the following values:</p> <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = Terminate</li> <li>• 2 = Request more quota</li> <li>• 3 = Redirect/Filter</li> </ul>

3

<b>TLV ID</b>	13 for Pool-ID
<b>Description</b>	This AVP identifies the resource pool that the quota included in this PPAQ is associated with.
<b>Length</b>	2+4

<b>Value</b>	Unsigned Integer representing a Pool-ID.
--------------	--

1

<b>TLV ID</b>	14 for Pool-Multiplier
<b>Description</b>	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. It consists of a Value-Digits field and optionally an Exponent field (as indicated by the length field).
<b>Length</b>	2+(8 or 12)
<b>Value</b>	<ul style="list-style-type: none"> <li>8 octets = Value-Digits field is an Unsigned64 value which contains the significant digits of the number. If decimal values are needed to present the units, the scaling <b>MUST</b> be indicated with the related Exponent field.</li> <li>4 octets = Exponent field is a Integer32 value which contains the exponent value to be applied for the Value-Digits field</li> </ul>

2

<b>TLV ID</b>	15 for Requested-Action
<b>Description</b>	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 <b>SHALL NOT</b> contain a Quota-Identifier, and <b>SHALL</b> contain a Service-ID 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.
<b>Length</b>	2+1
<b>Value</b>	Octet enumeration with the following values: <ul style="list-style-type: none"> <li>0 = Reserved</li> <li>1 = Balance Check</li> <li>2 = Price Enquiry</li> </ul>

3

<b>TLV ID:</b>	16 for Check-Balance-Result
<b>Description:</b>	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).
<b>Length:</b>	2+1
<b>Value:</b>	Octet enumeration with the following values: <ul style="list-style-type: none"> <li>0 = Success</li> <li>Any other value = Failure</li> </ul>

4

<b>TLV ID</b>	17 Cost-Information
<b>Description</b>	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 the Cost-Information AVP <b>SHALL NOT</b> appear in the response.

#### 1 5.4.2.38 Prepaid Tariff Switching Attribute (PTS)

11

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	TariffSwitchInterval	2+4	0	0-1	0	0
4	TimeIntervalAfterTariffSwitchUpdate	2+4	0	0-1[a]	0	0



**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.

<b>TLV ID</b>	1 for Quota Identifier
<b>Description</b>	Quota Identifier SHALL be included. In an online RADIUS Access-Request packet 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 of 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.
<b>Length</b>	2+4
<b>Value</b>	Octet String. The Quota Identifier value (most significant bit first)

<b>TLV ID</b>	2 for VolumeUsedAfterTariffSwitch
<b>Description</b>	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.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer representing a number of kilo-octets (1024 octets).

<b>TLV ID</b>	3 for TariffSwitchInterval
<b>Description</b>	Indicates the interval (in seconds) between the value of Event-Timestamp RADIUS attribute (see [40]) of the corresponding RADIUS Access-Request packet and the next tariff switch condition.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer indicating a number of seconds.

<b>TLV ID</b>	4 for TimeIntervalAfterTariffSwitchUpdate
<b>Description</b>	Contains the number of seconds of the tariff period that begins immediately after the period that ends as indicated by the TariffSwitchInterval 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.
<b>Length</b>	2+Length of Quota Identifier
<b>Value</b>	Unsigned Integer measuring a number of seconds.

#### 5.4.2.39 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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+---+---+---+---+---+

```

<b>WType-ID</b>	39 for Active-Time
<b>Description</b>	The amount of time the session was not in Idle state.
<b>Length</b>	6 + 3 +4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer. The time in seconds.

#### 5.4.2.40 hDHCP-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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	40 for hDHCP-RK
<b>Description</b>	The hDHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
<b>Length</b>	6 + 3 + 2(SALT) + length of the String containing the encrypted hDHCP-RK.
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2 octet SALT (see [39]) and String containing the encrypted hDHCP-RK formulated as per [39].

	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																																				
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	+-----+																																																																			

<b>WType-ID</b>	41 for hDHCP-RK-Key-ID
<b>Description</b>	An integer number uniquely identifying the hDHCP-RK within the scope of a single DHCP server.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit integer MSB first.

[illegible]

<b>WType-ID</b>	42 for hDHCP-RK-Lifetime
<b>Description</b>	Lifetime of the hDHCP-RK and derived keys.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

```

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      +-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

<b>WType-ID</b>	43 for DHCPMSG-Server-IP
<b>Description</b>	The IPv4 address of the DHCP server contained in the DHCPDISCOVER message.

<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv4 address of DHCP server (most significant bit first) to which the DHCPDISCOVER/DHCPREQUEST message was sent.

#### 5.4.2.44 Idle-Mode-Transition

```

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 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	44 for Idle-Mode-Transition
<b>Description</b>	A flag indicating whether the mobile node is in idle or not.
<b>Length</b>	6 + 3 + 1
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Octet. When set to (1) the MS is in idle mode. When set to (0) the MS is not in Idle mode.

#### 5.4.2.45 NAP-ID

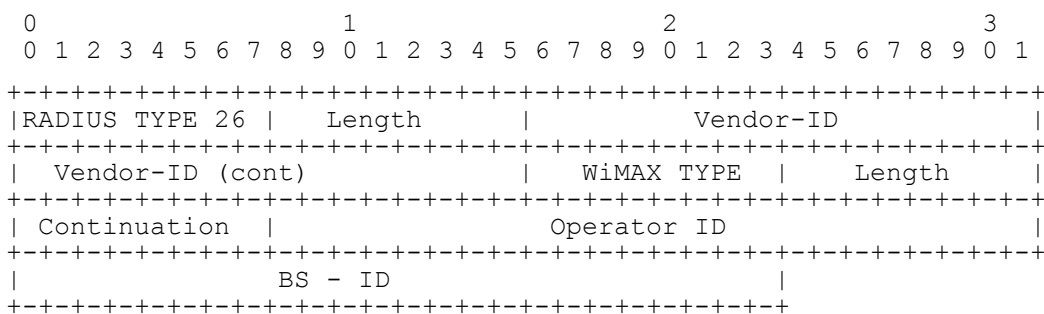
```

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 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

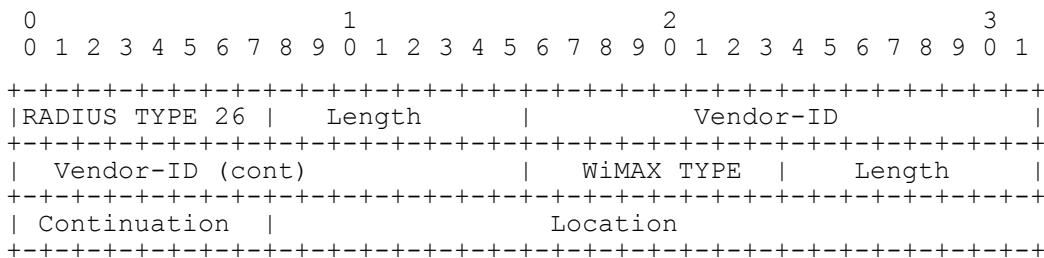
<b>WType-ID</b>	45 for NAP-ID
<b>Description</b>	Uniquely identifies the Network Access Provider.
<b>Length</b>	6 + 3 + 3
<b>Continuation</b>	C-bit = 0.
<b>Value</b>	Octet-String (3 Octets) representing an operator identifier.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12



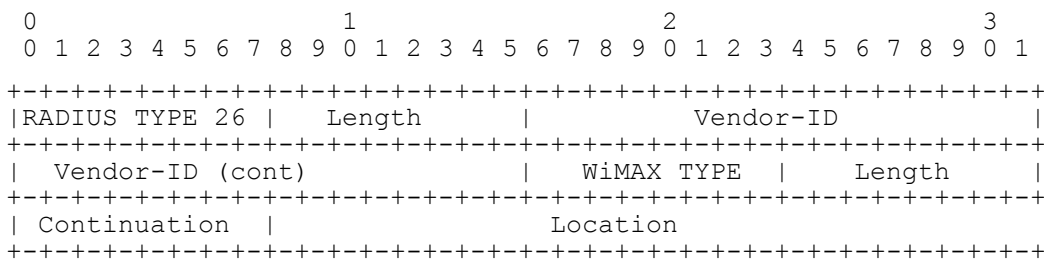
<b>WType-ID</b>	46 for BS-ID
<b>Description</b>	Uniquely identifies a NAP and a Base Station within that NAP.
<b>Length</b>	6 + 3 + 6
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet-String (6 Octets). Representing NAP operator identifier (first 3 Octets) and the Base Station ID (next 3 Octets).

13  
14  
15  
16  
17  
18  
19  
20  
21  
22



<b>WType-ID</b>	47 for Location
<b>Description</b>	Location of the ASN.
<b>Length</b>	6 + 3 + Length of Location ( >0)
<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	Octet-String representing location. Format is 0.

23  
24  
25  
26  
27  
28  
29  
30  
31  
32



<b>WType-ID</b>	48 for Acct- Input -Packets-Gigaword
<b>Description</b>	Number of packets incremented each time Acct- Input -Packets(47) overflows.

<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer representing $2^{32}$ packets counts.

#### 5.4.2.49 Acct- Output -Packets Gigaword

```

0
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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	49 for Acct- Output -Packets-Gigaword
<b>Description</b>	Number of packets incremented each time Acct- Output -Packets(48) overflows.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer representing $2^{32}$ packets counts.

#### 5.4.2.50 Uplink Flow Description

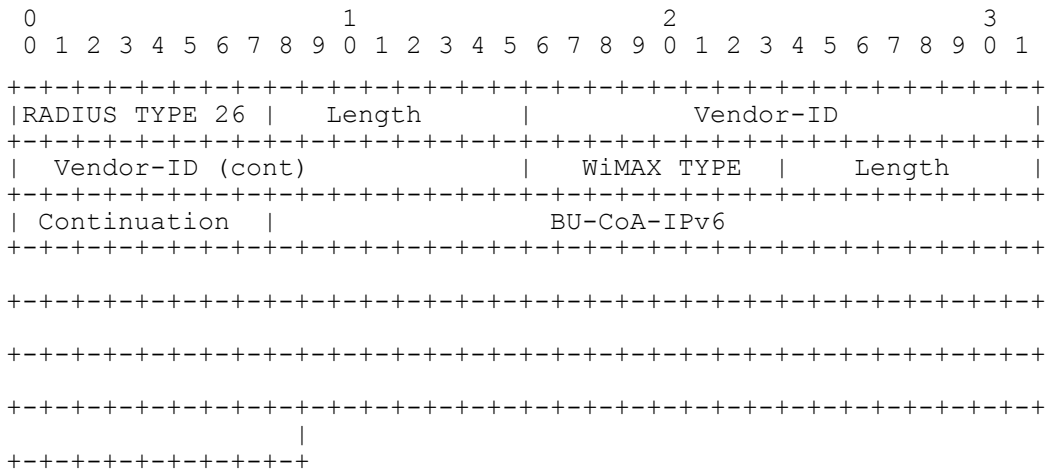
```

0
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 | Uplink Flow Description
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

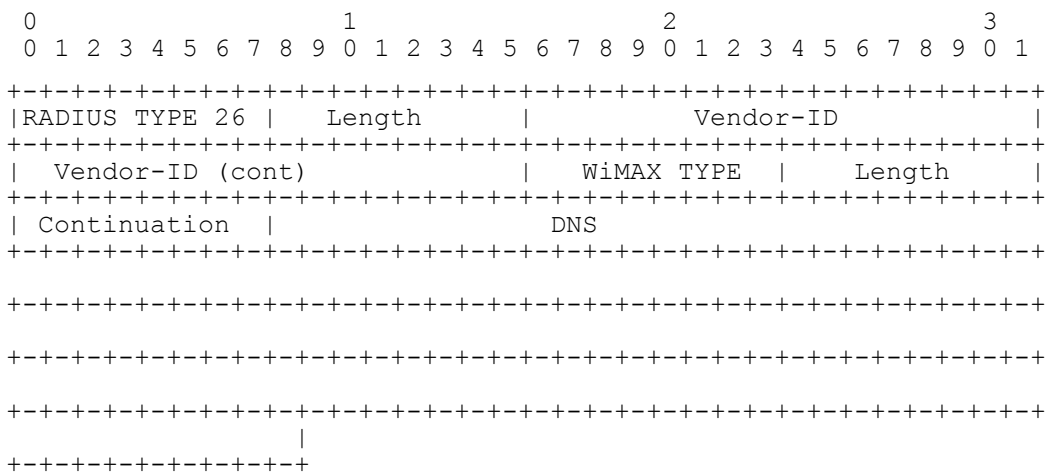
<b>WType-ID</b>	50 for Uplink Flow Description
<b>Description</b>	Describes an Uplink flow classifier.
<b>Length</b>	6+3 + Length of Uplink Flow Description
<b>Continuation</b>	C-bit = 0
<b>Value</b>	String containing an IP-Filter Rule as pre RFC3588. Action is set to "permit".

#### 5.4.2.51 BU-CoA-Ipv6



<b>WType-ID</b>	51 for BU-CoA-IPv6
<b>Description</b>	The CoA from the BU message.
<b>Length</b>	6 + 3 + 16
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet-String representing an IPv6 address most significant octet first.

#### 5.4.2.52 DNS



<b>WType-ID</b>	52 for DNS
<b>Description</b>	The IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.
<b>Length</b>	6 + 3 + (4 for IPv4 or 16 for IPv6)
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet-String representing an IPv4 or IPv6 address most significant octet first.

1

2  
3  
4  
5  
6  
7  
8  
9  
10

<b>WType-ID</b>	53 for Hotline-Profile-ID
<b>Description</b>	A unique identifier (relative to the HCSN) of a Hot-Line profile to be applied to this session.
<b>Length</b>	6 + 3 + length of octet-string.
<b>Continuation</b>	C-bit = 0
<b>Value</b>	<p>String representing a Hot-Line profile formatted as follows:  realm + "/" + profile-id-string</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• Realm is the Fully Qualified Domain Name of the operator that is asserting the Hot-Line profile; and</li> <li>• Profile-id-string is operator specific label for the Hot-Line profile to be applied at the by the Hot-Lining device.</li> </ul>

## 11

12  
13  
14  
15  
16  
17  
18  
19  
20

<b>WType-ID</b>	54 for HTTP-Redirection-Rule
<b>Description</b>	<p>An HTTP redirection rule. When the packet classifiers contained in this rule classifier matches protocol headers in a packet the NAS responds back with the specified URL causing the client's browser to be redirected to that URL. The HTTP redirection is expected to be supported using one of the application agnostic approaches such as HTTP status codes 3xx or Refresh Meta tag/HTTP refresh header. Application specific HTTP redirection methods such as JavaScript redirect which may cause inter-operability issues with roaming users are not recommended. Also, HTTP redirection only makes sense for inbound traffic from the MS to the ASN-GW. There SHALL NOT be any HTTP redirection rules specified on the outbound direction from the ASN-GW to the MS.</p> <p>When an HTTP request from a MS is redirected, it is quite possible that first redirect leads to another redirect if the packet classifiers in the HTTP redirection rule happen to match the IP destination resolved from the redirect URL. This behavior is called “redirect loop”. If there is no other HTTP redirect rule to break the “redirect loop”, the NAS and MS can end up in an infinite loop of redirects until the MS browser detects this situation, stops further HTTP requests, and display an error message to the user. For example, the</p>



	<p>following HTTP redirection rule forces any HTTP requests from the MS to <a href="http://www.wimaxforum.org/home">http://www.wimaxforum.org/home</a>:  redirect <a href="http://www.wimaxforum.org">http://www.wimaxforum.org</a> in ip from assigned to any 80</p> <p>The first redirect results in the MS browser sending the original HTTP request to 66.179.20.189, which is the IP for <a href="http://www.wimaxforum.org">http://www.wimaxforum.org</a>. But this redirected HTTP request will generate IP packet that triggers another redirect to the same URL, <a href="http://www.wimaxforum.org">http://www.wimaxforum.org</a> again, as the “any” destination in the above HTTP redirect rule matches any IP destination address including 66.179.20.189. This will lead into an infinite loop of redirects until the MS browser detects the “redirect loop”.</p> <p>In order to avoid the HTTP redirection loops, the following requirements need to be met during the provisioning of HTTP redirection rules:</p> <ol style="list-style-type: none"> <li>1. When an HTTP redirection rule contains a “wildcard” packet classifier that can match any destination address, an explicit pass rule must precede this HTTP redirection rule in the MS Hot-Lining profile. The following two rules would guarantee the correct HTTP redirection for the above example:  pass in ip from assigned to 66.179.20.0/8 80  redirect <a href="http://www.wimaxforum.org">http://www.wimaxforum.org</a> in ip from assigned to any 80</li> <li>2. When an HTTP redirection rule contains a subnet prefix packet classifier for destination and a redirect URL that can be resolved in an IP in the same destination subnet, an explicit pass rule must precede this HTTP redirection rule in the MS Hot-Lining profile. For example,  pass in ip from assigned to 66.179.20.189 80  redirect <a href="http://www.wimaxforum.org">http://www.wimaxforum.org</a> in ip from assigned to 66.179.20.0/8 80</li> </ol>								
<b>Length</b>	6 + 3 + length of rule.								
<b>Continuation</b>	C-bit = 0								
<b>Value</b>	<p>An string formatted as per IPFilterRule specified by [54] with the following exception:  The action portion of the rule SHALL follow the following:</p> <table border="1"> <thead> <tr> <th>Action Keyword</th><th>Description</th></tr> </thead> <tbody> <tr> <td>"redirect" url</td><td>If the rule matches then redirect packets that match the rule to the specified URL encoded as per RFC2396</td></tr> <tr> <td>"pass"</td><td>If the rule matches then the HTTP request is allowed to continue through. The is no url.</td></tr> <tr> <td>"flush"</td><td>Has no other elements in the rule. The Hot-Lining device SHALL flush all HTTP-Redirection rules received from the HAAA.</td></tr> </tbody> </table>	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 Hot-Lining device SHALL flush all HTTP-Redirection rules received from the HAAA.
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 Hot-Lining device SHALL flush all HTTP-Redirection rules received from the HAAA.								

#### 5.4.2.55 IP-Redirection-Rule

```

1
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     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	55 for IP Redirection Rule.		
<b>Description</b>	The IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.		
<b>Length</b>	6 + 3 + length of rule		
<b>Continuation</b>	C-bit = 0		
<b>Value</b>	An string formatted as per IPFilterRule specified by [54] 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 Hot-Lining device SHALL flush all HTTP-Redirection rules received from the HAAA.	

#### 5.4.2.56 Hotline-Session-Timer

```

1
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 | unsigned integer
10     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
11     |
12     +---+---+---+---+---+

```

<b>WType-ID</b>	56 for Hotline-Session-Timer		
<b>Description</b>	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.		
<b>Length</b>	6 + 3 + 4		
<b>Continuation</b>	C-bit = 0		
<b>Value</b>	Unsigned Integer representing a time in seconds. A value of zero means infinity.		

#### 5.4.2.57 NSP-ID

```

13
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 | Operator ID
22     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	57 for NSP-ID
<b>Description</b>	Uniquely identifies the Network Service Provider.
<b>Length</b>	6 + 3 + 3
<b>Continuation</b>	C-bit = 0.
<b>Value</b>	Octet-String (3 Octets) representing an operator identifier.

#### 5.4.2.58 Void

#### 5.4.2.59 Count-Type

```

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          |
+-----+-----+-----+-----+-----+-----+-----+

```

<b>WType-ID</b>	59 for Count-Type
<b>Description</b>	Used to indicate if the record represents compressed or uncompressed counts.
<b>Length</b>	6 + 3 + 1
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Octet. When set to (0) indicates uncompressed counts. When set to (1) indicates compressed counts.

#### 5.4.2.60 WiMAX-DM-Action-Code

```

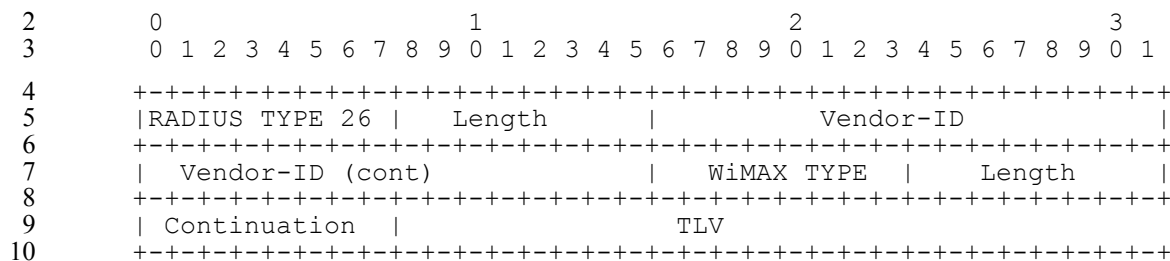
0                               1                               2                               3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-----+-----+-----+-----+-----+-----+-----+-----+
|RADIUS TYPE 26 | Length          | Vendor-Id          |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Vendor-Id (cont) | WiMAX TYPE | Length          |
+-----+-----+-----+-----+-----+-----+-----+-----+
| Continuation | WiMAX DM Action Code |
+-----+-----+-----+-----+-----+-----+-----+-----+
| |
+-----+-----+-----+-----+-----+-----+-----+

```

<b>WType-ID</b>	60 for WiMAX-DM-Action-Code
<b>Description</b>	This attribute indicates the deregistration action to take when the NAS receives a Disconnect Message.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Integer. Enumerator. The values are: <ul style="list-style-type: none"> <li>0x0000 = Deregister MS. MS SHALL immediately terminate service with the BS and should attempt network entry at another BS.</li> <li>0x0001 = Suspend all MS traffic including control traffic. MS SHALL listen to the</li> </ul>

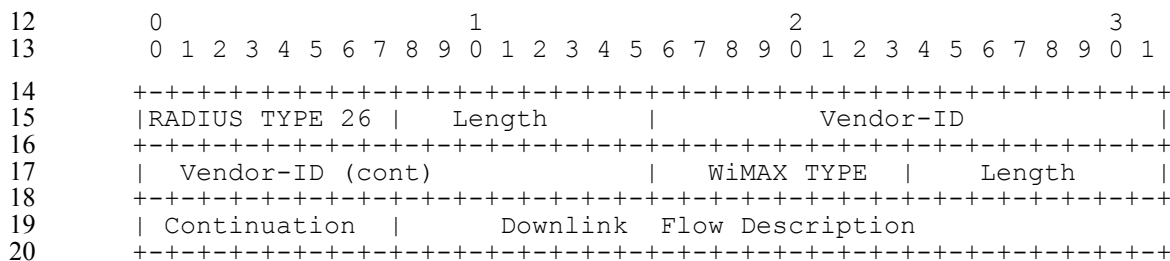
	<p>current BS but SHALL NOT transmit until an RES-CMD message or DREG-CMD with Action Code 02 or 03 is received.</p> <ul style="list-style-type: none"> <li>• 0x0002 = Suspend user traffic (transport connections). MS SHALL listen to the current BS but only transmit on the Basic and Primary Management Connections.</li> <li>• 0x0003 = Resume traffic. MS SHALL return to normal operation and may transmit on any of its active connections.</li> <li>• 0x0004 = Reserved.</li> <li>• 0x0005 = MS SHALL be put into idle mode.</li> <li>• 0x0006 = MS successfully completed MIP6 handover.</li> <li>• 0xFFFF = MS SHALL be sent the RES-CMD by the BS. The MS will reload all configuration information and do initial network entry.</li> <li>• 0x0007 - 0xFFFE = Reserved.</li> </ul>
--	--

#### 5.4.2.61 FA-RK-SPI



<b>WType-ID</b>	61 for FA-RK-SPI
<b>Description</b>	The SPI used for the FA-RK.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit integer MSB first.

#### 5.4.2.62 Downlink Flow Description



<b>WType-ID</b>	62 for Downlink Flow Description
<b>Description</b>	Describes a flow classifier for the downlink.
<b>Length</b>	6+3 + Length Downlink Flow Description
<b>Continuation</b>	C-bit = 0
<b>Value</b>	String containing an IP-Filter Rule as pre RFC3588. Action is set to "permit".

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	2	3	4	5	6	7	8	9	0	1
RADIUS TYPE 26										Length										Vendor-ID																					
Vendor-ID (cont)										WiMAX TYPE										Length																					
Continuation										QoS Descriptor																															

<b>WType-ID</b>	63 for Downlink-Granted-QoS
<b>Description</b>	Downlink QoS granted to the MS.
<b>Length</b>	6+3 + Length of QoS-Descriptor
<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	QoS Descriptor value

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	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																															

<b>WType-ID</b>	64 for vHA-IP-MIP4
<b>Description</b>	The IPv4 address of the vHA for MIP4.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv4 address (most significant bit first).

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	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																															

<b>WType-ID</b>	65 for vHA-IP-MIP6
<b>Description</b>	The IPv6 address of the vHA for MIP6.
<b>Length</b>	6 + 3 + 16
<b>Continuation</b>	C-bit = 0

<b>Value</b>	Octet string containing an IPv6 address (most significant bit first).
--------------	---

#### 5.4.2.66 MN-vHA-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          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	66 for MN-vHA-MIP4-KEY
<b>Description</b>	The MN-vHA-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 Visited HA to validate the MN-HA-AE (CMIP4) and to compute the MN-HA-AE for of the CMIP4 Registration Response and the SPI.
<b>Length</b>	6 + 3 +2(SALT)+ Length of the encrypted MN-vHA-MIP4-KEY
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2 octet SALT (see [39]) and String containing the encrypted MN-vHA-MIP4-KEY formulated as per [39].

#### 5.4.2.67 vHA-RK-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          |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	67 for vHA-RK-KEY
<b>Description</b>	The vHA-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.
<b>Length</b>	6 + 3 + 2(SALT) + length of the String containing the encrypted vHA-RK-KEY.
<b>Continuation</b>	When following the procedures defined in [39] if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2-octet SALT (see [39]) and String containing the encrypted vHA-RK formulated as per [39].

1

2  
3  
4  
5  
6  
7  
8  
9  
10

<b>WType-ID</b>	68 for vHA-RK-SPI
<b>Description</b>	The SPI used for the vHA-RK.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit integer MSB first.

## 11

12  
13  
14  
15  
16  
17  
18  
19  
20

<b>WType-ID</b>	69 for vHA-RK-Lifetime
<b>Description</b>	The Lifetime of the vHA-RK and derived keys.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit integer MSB first representing the time before the key expires in seconds.

## 21

22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32

<b>WType-ID</b>	71 MN-vHA-MIP4-SPI
<b>Description</b>	The SPI associated with the MN-vHA-MIP4-KEY.

<b>Length</b>	6+3+4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit Integer. In an Access-Accept sent from the home AAA to the ASN the value is set to SPI-PMIP4.

#### 5.4.2.71 vDHCPv4-Server

```

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 | vDHCP-Server IPv4
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	73 for vDHCPv4-Server
<b>Description</b>	The IPv4 address of the visited DHCP-Server to use for IPv4 address allocation by the vASN.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv4 address (most significant bit first).

#### 5.4.2.72 vDHCPv6-Server

```

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 | vDHCP-Server IPv6
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	74 for vDHCPv6-Server
<b>Description</b>	The IPv6 address of the visited DHCP-Server to use for IPv6 allocation by the vASN.
<b>Length</b>	6 + 3 + 16
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv6 address (most significant bit first).



### 5.4.2.73 vDHCP-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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	75 for vDHCP-RK
<b>Description</b>	The vDHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
<b>Length</b>	6 + 3 + 2(SALT) + length of the String containing the encrypted vDHCP-RK.
<b>Continuation</b>	When following the procedures defined in [39], if the resulting encrypted string will be greater than 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.
<b>Value</b>	The value consists of 2 octets for the SALT (see [39]) And a String containing the encrypted vDHCP-RK formulated as per [39].

### 5.4.2.74 vDHCP-RK-Key-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 | Key ID of the vDHCP-RK
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	76 for vDHCP-RK-Key-ID
<b>Description</b>	An integer number uniquely identifying the vDHCP-RK within the scope of a single DHCP server.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit integer MSB first.

#### 5.4.2.75 vDHCP-RK-Lifetime

```

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 | Lifetime of the vDHCP-RK
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	77 for vDHCP-RK-Lifetime
<b>Description</b>	Lifetime of the vDHCP-RK and derived keys.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

#### 5.4.2.76 PMIP-Authenticated-Network-Identity

```

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 | NAI
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	78 for PMIP-Authenticated-Network-Identity
<b>Description</b>	Authenticated identity of the MS.
<b>Length</b>	6+3 + length of NAI
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing Identity of the MS in NAI format.

#### 5.4.2.77 Visited-Framed-IP-Address

```

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 | Visited-Framed-IP-Address
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	79 for Visited-Framed-IP-Address
<b>Description</b>	The IPv4 Address assigned by the Visited CSN to be used for the MS.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0

<b>Value</b>	Octet string containing an IPv4 address (most significant bit first).
--------------	---

#### 5.4.2.78 Visited-Framed-IPv6-Prefix

```

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 | Prefix-Length | Visited-Framed-IPv6-Prefix
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	80 for Visited-Framed-IPv6-Prefix
<b>Description</b>	The IPv6 prefix assigned by the Visited CSN to be used for the MS.
<b>Length</b>	(6 + 3) + 1 + (0-16)
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string contains one byte of “Prefix-Length” and up to 16 bytes of Visited-Framed-IPv6-Prefix.

#### 5.4.2.79 Visited-Framed-Interface-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 | Visited-Framed-Interface-Id
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	81 for Visited-Framed-Interface-Id
<b>Description</b>	The IPv6 interface Id assigned by the Visited CSN to be used for the MS.
<b>Length</b>	6 + 3 + 8
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing an IPv6 address (most significant bit first)

#### 5.4.2.80 MIP-Authorization-Status

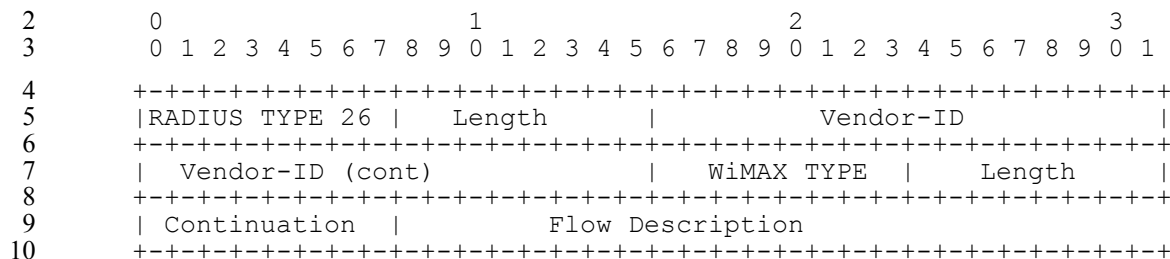
```

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 | MIP-Authorization-Status Flag
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|                               |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

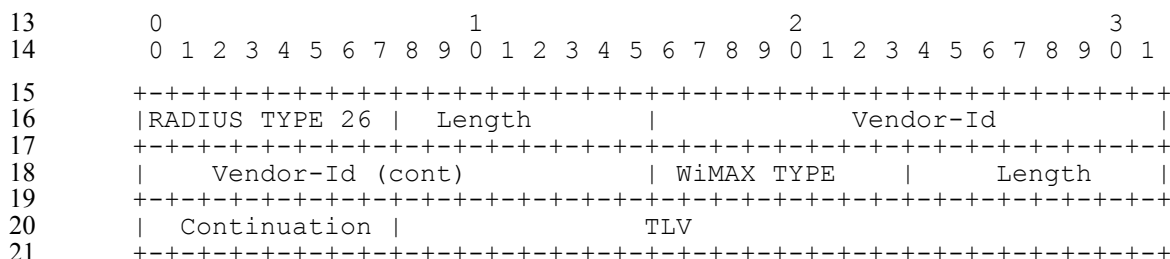
<b>WType-ID</b>	82 for MIP-Authorization-Status
<b>Description</b>	This attribute when set to ‘true’ means AAA is authorizing the MS to use MIP6. ‘False’ means the MS is not authorized.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	The value is an unsigned 32-bit integer. If the value is set to 1 (TRUE) then the AAA has authorized the MS to use MIP6. If the value is set to 0 (FALSE) then the AAA has not authorized the MS to use MIP6.

#### 5.4.2.81 Flow-Description-V2



<b>WType-ID</b>	83 for Flow-Description-V2
<b>Description</b>	Describes a classifier of a flow.
<b>Length</b>	6+3 + Length of classifier TLV
<b>Continuation</b>	C-bit = 0
<b>Value</b>	A classifier encoded using TLVs as described in section 5.4.2.84.

#### 5.4.2.82 Packet-Flow-Descriptor-V2



<b>WType-ID</b>	84 for Packet-Flow-Descriptor-V2
<b>Description</b>	<p>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.</p> <p>In case of COA message, the complete QoS-context should be transferred and will replace the existing one in ASN. A SF modification followed by an accounting-request with the updates can be performed by the ASN if a PacketDataFlowID matches with the previous ID. PacketDataFlows which are not present anymore SHALL be deleted. New PacketDataFlows should be created according to the provided parameters. Corresponding accounting-requests SHALL be generated.</p>
<b>Length</b>	6 + 3 + TLVs

<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	The sub-types described below.

1

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	Classifier <sup>33</sup>	2+Length	0	0-n	0	0
10	Paging-Preference	2+1	0	0-1[e]	0	0
11	VLANTagProcessingRuleID	2+2	0	0-1[f]	0	0

## 2 Notes:

- [a] If ServiceProfileID is provided then TLV IDs greater than 3 overrides the QoS parameter settings of the related ServiceProfile according to the TLV-value. The order in which the Packet-Flow-Descriptor will be mapped to the pre-configured flows at the ASNGW SHALL be the same in which they are received.
- [b] If ServiceProfileID is not provided these RADIUS attributes are MANDATORY. If the RADIUS attributes are missing then the NAS SHALL silently discard this RADIUS attribute and should reject the network entry of the MS.
- [c] This attribute SHALL be present if ServiceProfileID is not present and:  
Direction is Uplink or  
Direction is bi-directional and the flow is symmetrical or not symmetrical.  
If the attribute is missing then the NAS SHALL reject the network entry of the MS.
- [d] This attribute SHALL be present if ServiceProfileID 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.
- ([e]) This attribute is applicable to the downlink service flow only.
- [f] This attribute may only be present for Ethernet service flows.

3

<sup>33</sup> Classifier defined within Packet Flow Descriptor maps to “Classification Rule” defined over R4/R6 interfaces

<b>TLV ID</b>	1 for PacketDataFlow-ID
<b>Description</b>	This attribute 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 assigned for the packet data flow of the Initial Service Flow (ISF).
<b>Length</b>	2+2
<b>Value</b>	Unsigned Short representing the flow identifier (most significant bit first). A value of zero(0) is invalid.

1

<b>TLV ID</b>	2 for ServiceDataFlow-ID
<b>Description</b>	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 assigned for the Initial Service Flow.
<b>Length</b>	2+2
<b>Value</b>	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.

2

<b>TLV ID</b>	3 ServiceProfileID
<b>Description</b>	This attribute identifies a pre-configure flow descriptor at the NAS.
<b>Length</b>	2+4
<b>Value</b>	Unsigned Integer representing the identity of a Flow Spec that is pre-provisioned (most significant bit first). A value of zero(0) is invalid.

3

<b>TLV ID</b>	4 for Direction
<b>Description</b>	The direction of the Packet Data Flow.
<b>Length</b>	2+1
<b>Value</b>	Octet enumeration with the following values: <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = Uplink</li> <li>• 2 = Downlink</li> <li>• 3 = Bi-directional</li> <li>• 4 – FF = Reserved</li> </ul>

4

<b>TLV ID</b>	5 for ActivationTrigger
<b>Description</b>	This parameter specifies the trigger to be used for the activation of the service flow. For the ISF, Provisioned, Admit and Activate SHALL be set. The Activate SHALL be mandatorily supported by the ASN. All other states need not to be supported in Rel1.0 and should be interpreted as "Activate" if not supported.

<b>Length</b>	2+1
<b>Value</b>	<p>Octet bit-map with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 - Provisioned (SHALL be set in case of ISF)</li> <li>• Bit #1 - Admit (SHALL be set in case of ISF)</li> <li>• Bit #2 - Activate (SHALL be set in case of ISF)</li> <li>• Bit #3 - Dynamic Reservation (not valid for ISF)</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p> <p>If “Dynamic Reservation” is set to false, the QoS-Descriptor is used to specify a QoS profile for ISFs or pre-provisioned SFs.</p> <p>If “Dynamic Reservation” is set to true, the QoS-Descriptor is used to specify a QoS profile for authorization checks done by the Anchor-SFA.</p>

1

<b>TLV ID</b>	6 for TransportType
<b>Description</b>	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].
<b>Length</b>	2+1
<b>Value</b>	<p>Octet enumeration with the following values:</p> <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = IPv4-CS</li> <li>• 2 = IPv6-CS</li> <li>• 3 = Ethernet</li> <li>• 4 – 255 = Reserved</li> </ul>

2

<b>TLV ID</b>	7 for UplinkQoSID
<b>Description</b>	<p>The identifier of the QoS descriptor for the uplink direction or for bi-direction if the flow is bi-directional with symmetrical QoS.</p> <p>If the QoSID is not resolvable by the NAS, the NAS SHALL reject the network entry of the MS.</p>
<b>Length</b>	2+1
<b>Value</b>	Unsigned Octet containing the ID of the QoS descriptor.

3

<b>TLV ID</b>	8 for DownlinkQoSID
<b>Description</b>	<p>The identifier of the QoS descriptor for the downlink direction.</p> <p>If the QoSID is not resolvable by the NAS, the NAS SHALL reject the network entry of the MS.</p>
<b>Length</b>	2+1
<b>Value</b>	Unsigned Octet containing the ID of the QoS descriptor.

4

<b>TLV ID</b>	9 for Classifier
<b>Description</b>	The classifier to match for traffic flowing in the direction indicated by the direction encoded in the classifier. Classifiers for the appropriate direction are evaluated in order, with the first matched rule terminating the evaluation. If the classifier cannot be parsed then the NAS SHALL reject the network entry of the MS.
<b>Length</b>	2+Variable
<b>Value</b>	Contains a set of nested TLVs describing IP classifiers.

1

<b>TLV ID</b>	10 for Paging-Preference
<b>Description</b>	This parameter is a single bit indicator of an MS's preference for the reception of paging advisory messages during idle mode. When set, it indicates that the BS may present paging advisory messages or other indicative messages to the MS when data SDUs bound for the MS are present while the MS is in idle mode.
<b>Length</b>	2+1
<b>Value</b>	Refer to 802.16e section 11.13.30.

2

<b>TLV ID</b>	11 for VLANTagProcessingRuleID
<b>Description</b>	The ID of the rules for assigning priority bits and VLAN-IDs in Ethernet frames
<b>Length</b>	2+2
<b>Value</b>	Unsigned-Short containing the VLANTagProcessingRuleID of the rules for processing the VLAN tags in Ethernet frames

3

#### 5.4.2.83 Classifier

4

```

5      0          1          2          3
6      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
7      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
8      | TLV-ID 9 or 10 | LENGTH          | TLV-ID 1 | LENGTH = 3 |
9      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
10     | classifier id | TLV-ID 2          | LENGTH = 3 | protocol   |
11     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
12     | TLV-ID 3      | LENGTH = 3 | direction   | . . . . .
13     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

13

TLV ID	TLV Name	Length Octets	Occurrence
1	ClassifierID	2+1	1[a]
2	Priority	2+1	1[a]
3	Protocol	2+1	0-1
4	Direction	2+1	1
5	Source-Specification	2+Variable	0-1
6	Destination-Specification	2+Variable	0-1



TLV ID	TLV Name	Length Octets	Occurrence
7	IP TOS/DSCP Range and Mask	2+3	0-1
8	Action	2+1	1
9	ETH-Option	2+Variable	0-1[b]

1 Notes:

[a] Classifier ID is unique within the parent container.

[b] May only present in case of Ethernet based transport.

2

<b>TLV ID</b>	1 for Classifier ID
<b>Description</b>	An identifier of the classifier that uniquely identifies the classifier in the scope of the Packet-Flow-Descriptor irrespective of whether or not the classifier is an uplink or downlink classifier.
<b>Length</b>	2+1
<b>Value</b>	0 to 255.

3

<b>TLV ID</b>	2 for Priority
<b>Description</b>	The value of the field specifies the priority for processing this classifier relative to other classifiers. It is expected to be unique across all packet data flows for a given direction (uplink/downlink). A bidirectional packet data flow can be considered as both uplink and downlink.
<b>Length</b>	2+1
<b>Value</b>	Unsigned 8-bit integer. The higher the value the higher the priority.

4

<b>TLV ID</b>	3 for Protocol
<b>Description</b>	The value of the field specifies a matching value 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.
<b>Length</b>	2+1
<b>Value</b>	Unsigned 8-bit integer. The encoding of the value field is that defined by the IANA document "Protocol Numbers."

5

<b>TLV ID</b>	4 for Direction
<b>Description</b>	Specifies the direction of the classifier. IN is from the terminal and OUT is to the terminal. Bi-direction means that the classifier applies to traffic in both directions. In the case of the direction is Bi-directional and we are comparing packets coming from the IN direction(from the terminal) then the orientation of the Source and Destination specification is correct. When comparing packet coming from the OUT direction(towards the terminal) then the orientation of the Source and Destination specification must be swapped. That is the Source fields of the packet are compared to the Destination

	specification of the classifier and the Destination fields of the packet are compared to the Source specification of the classifier.
<b>Length</b>	2+1
<b>Value</b>	Octet enumeration with the following values: <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = IN (from the terminal)</li> <li>• 2 = OUT (to the terminal)</li> <li>• 3 = Bi-directional</li> <li>4 – FF = Reserved.</li> </ul>

1

<b>TLV ID</b>	5 for Source-Specification
<b>Description</b>	Contains a source specification for a packet. When the direction attribute is set to bi-direction the Source Specification is compared to the Source field of the IN coming packets and the Destination field of the OUT going packets. If this field is omitted, then comparison of the source IP and port or source MAC address for this entry is irrelevant.
<b>Length</b>	2+Variable
<b>Value</b>	Contains a nested TLV describing a source specification.

2

<b>TLV ID</b>	6 for Destination-Specification
<b>Description</b>	Contains a destination specification for a packet. When the direction attribute is set to bi-direction the Destination Specification(s) is compared to the Destination field of the IN coming packets and the Source field of the OUT going packets. If this field is omitted, then comparison of the destination IP and port or destination MAC address for this entry is irrelevant.
<b>Length</b>	2+Variable
<b>Value</b>	Contains a nested TLV describing a destination specification.

3

<b>TLV ID</b>	7 for IP TOS/DSCP Range and Mask
<b>Description</b>	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.
<b>Length</b>	2+3
<b>Value</b>	The first octet represents the lower limit of the ToS, the second octet represents the higher limit of the ToS and the last octet represents the mask value.

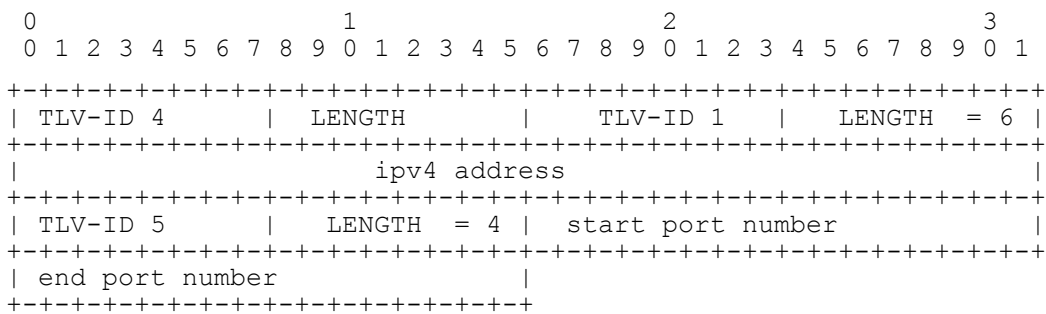
4

<b>TLV ID</b>	8 for Action
---------------	--------------

<b>Description</b>	The value of this field specifies the action to either allow packets that match the rule or drop packets that match the rule.
<b>Length</b>	2+1
<b>Value</b>	Octet enumeration with the following values: <ul style="list-style-type: none"> <li>0 = Reserved</li> <li>1 = Permit – Allow Packets that match the rule.</li> <li>2 = Deny – Drop packets that match the rule.</li> <li>3 – FF = Reserved</li> </ul>

<b>TLV ID</b>	9 for ETH Option
<b>Description</b>	A grouped TLV with Ethernet specific attributes.
<b>Length</b>	2+Variable
<b>Value</b>	Contains a set of nested TLVs describing the Ethernet specific classifiers.

#### 5.4.2.84 Source/Destination Specification



TLV ID	TLV Name	Length Octets	Occurrence
1	IPAddress	2+4 or 2+16	0-1[a]
2	IPAddressRange	2+8 or 2+32	0-1[a][d]
3	IPAddressMask	2+8 or 2+32	0-1[a]
4	Port	2+2	0-n[b][d]
5	PortRange	2+4	0-n[b]
6	Inverted	2+1	0-1[c][d]
7	Assigned	2+1	0-1[d]
8	MACAddress	2+6	0-1[e]
9	MACMask	2+6	0-1[e]

Notes:

- [a] Only one of IPAddress, IPAddressRange, IPAddressMask may appear in a source specification. If the IP address TLVs are missing then comparison of the IP address field is irrelevant.
- [b] If one of the Port(s) matches, there is no need to check the PortRange; or if one of the PortRange(s) matches, then there is no need to check the Ports. The order of checking SHALL be in the order that they appear in the container. If the port TLVs are missing then comparison of the port field is irrelevant.
- [c] Inverted inverts the notion of the IP address fields (1,2,3 and 7). It does not impact the port or port range specification. Inverted MAY only appear when one or more of the IP Address fields (1,2,3 and 7) appear. Otherwise the source/destination specification is in error.
- [d] This attribute is used only by the network for downlink traffic. It is not sent to the MS.
- [e] Only valid for ETH-CS.

1

<b>TLV ID</b>	1 for IPAddress
<b>Description</b>	Specifies an IPv4 or IPv6 address to match. Zero or more IP addresses can be specified in a source or destination specification. IPv4 and IPv6 addresses must not be both specified.
<b>Length</b>	2+4 octets for IPv4 Address or 2+ 16octets for IPv6 address
<b>Value</b>	A value representing an IPv4 address or an IPv6 address.

2

<b>TLV ID</b>	2 for IPAddressRange
<b>Description</b>	Specifies and IPv4 or an IPv6 address range to match. The range is inclusive. Zero or more IP address ranges may appear in the Source or Destination specification. Both values MUST be IPv4 or IPv6.
<b>Length</b>	2+8 for IPv4 Address range or 2+32 for IPv6 Address range
<b>Value</b>	The first 4 or 16 octets represent the start of the IP range and the second 4 or 16 octets represent the end of the range inclusively.

3

<b>TLV ID</b>	3 for IPAddressMask
<b>Description</b>	Represents a block of IPv4 or IPv6 addresses as a base plus a bit-width mask. For example 1.2.3.4/24 is encoded by encoding the ip address 1.2.3.4 to a 32-bit value and setting the last octet to 24. In this case all ip addresses in the range of 1.2.3.0 to 1.2.3.255 will match. An IPAddressMask representing 0.0.0.0/0 matches ANY IPv4 address. Similarly 0::/0 matches ANY IPv6 address.
<b>Length</b>	2+5 For IPv4 block of addresses or 2+17 for an IPv6 block of addresses.
<b>Value</b>	The first 4 or 16 octets represent the base IPv4 or IPv6 address, the last octet represents the bit-width mask. The bit-width mask must be valid for the type of IP address.

4

<b>TLV ID</b>	4 for Port
<b>Description</b>	Represent an IP port.
<b>Length</b>	2+2 Octets
<b>Value</b>	16-bit unsigned integer representing port numbers.

1

<b>TLV ID</b>	5 for Port Range
<b>Description</b>	Represents an inclusive port range consisting of a start port and an end port.
<b>Length</b>	2+4 Octets
<b>Value</b>	The first 2 octets represent the start of the port range and the second of the 2 octets represents the end of the port range inclusively.

2

<b>TLV ID</b>	6 for Inverted
<b>Description</b>	If not present or set to false (0) then the IP address specification proceeds as follows an IP match is found if any of the IP fields (1,2,3) match the IP address in the packet. The IP fields are ORed together. Matches if IP Address matches: IPAddress1 or IPAddress2 or IPAddressRange1 or IPAddressMask1.If present and set to true (1) then the IP address specification proceeds as follows: the IP fields are inverted and are ANDed together. Matches if IP Address is: NOT IPAddress1 AND NOT IPAddress2 AND NOT IPAddressRange1 AND NOT IPAddressMask1.
<b>Length</b>	2+1
<b>Value</b>	One octet representing boolean. 0 for false, 1 for true.

3

<b>TLV ID</b>	7 for Assigned
<b>Description</b>	If present indicates to use the assigned address(es) for the mobile in the source specification or destination specification or both.
<b>Length</b>	2+1 octets
<b>Value</b>	Unsigned 8-bit enumeration with values defined as follows: <ul style="list-style-type: none"> <li>• 1 indicating the Source Assigned</li> <li>• 2 indicating the Destination Assigned</li> <li>• 3 indicates Source and Destination Assigned</li> </ul> Other values are reserved.

4

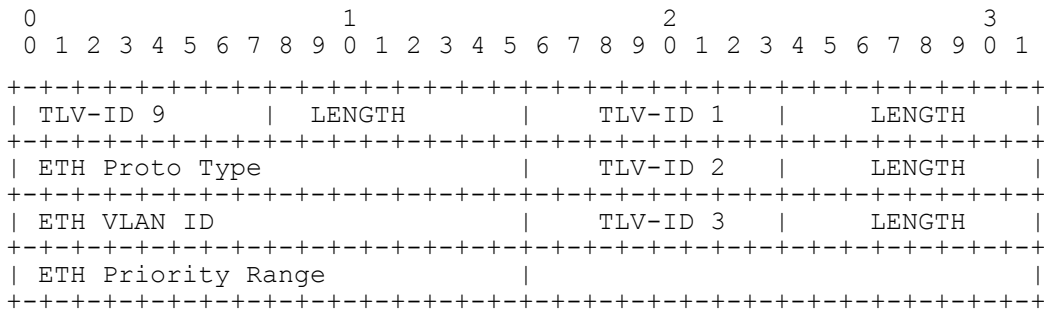
<b>TLV ID</b>	8 for MAC address
<b>Description</b>	The value of this field specifies the MAC address
<b>Length</b>	2+6
<b>Value</b>	A value representing a MAC address

5

<b>TLV ID</b>	9 for MAC mask
<b>Description</b>	The value of this field specifies the MAC mask
<b>Length</b>	2+6
<b>Value</b>	A value representing a MAC mask

6

#### 5.4.2.85 ETH Option



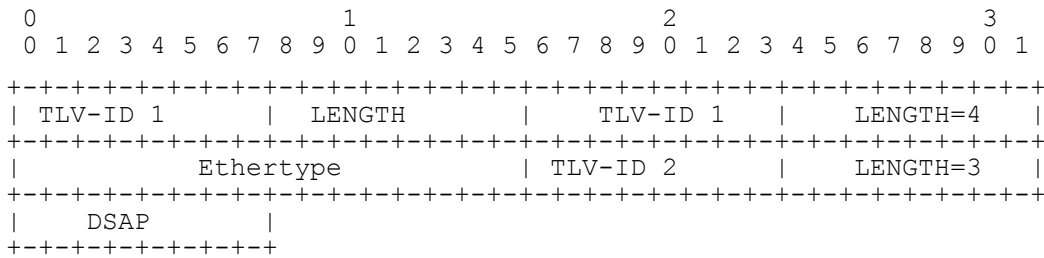
TLV ID	TLV Name	Length Octets	Occurrence
1	ETH Proto Type	2+Variable	1
2	ETHVLAN ID	2+Variable	0-1
3	ETH Priority Range	2+Variable	0-n

<b>TLV ID</b>	1 for ETH Proto Type
<b>Description</b>	Specifies Ethertype and DSAP.
<b>Length</b>	2+Variable
<b>Value</b>	Contains a nested TLV describing ETH Protocol Type

<b>TLV ID</b>	2 for ETH VLAN ID
<b>Description</b>	If present, this field specifies the matching values for the VLAN-ID bits. If omitted, the VLAN-ID bits are irrelevant for this entry.
<b>Length</b>	2+Variable
<b>Value</b>	Contains a nested TLV describing the VLAN-ID.

<b>TLV ID</b>	3 for ETH Priority Range
<b>Description</b>	If present, the priority SHALL match to the packet as specified in IEEE802.1D
<b>Length</b>	2+Variable
<b>Value</b>	Contains a set of nested TLVs describing the Ethernet Priority.

#### 5.4.2.86 ETH Proto Type



TLV ID	TLV Name	Length Octets	Occurrence
1	Ethertype	2+2	0-n[a]
2	DSAP	2+1	0-n[a]

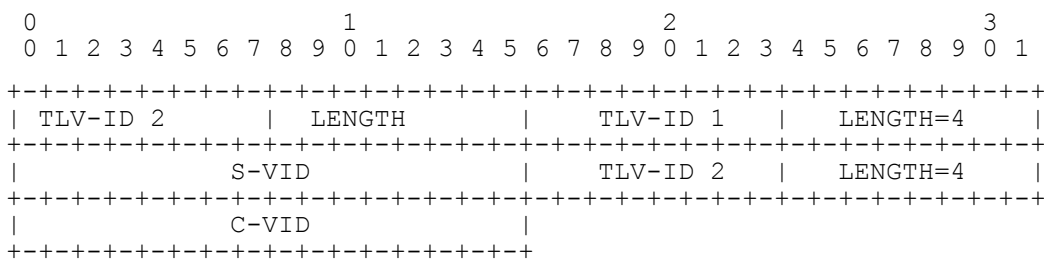
Notes:

[a] Both might be absent. Only one of them is allowed to be present.

<b>TLV ID</b>	1 for ETH Ethertype
<b>Description</b>	Applies to Ethertype value contained in packets using DEC-Intel-Xerox (DIX) encapsulation or the Sub-Network Access Protocol (SNAP) encapsulation (IEEE802.2, RFC1042) format.
<b>Length</b>	2+2 octets
<b>Value</b>	16 bit representation of the Ethertype which SHALL match with the target.

<b>TLV ID</b>	2 for DSAP
<b>Description</b>	Specifies the Destination Service (DSAP) when SDUs using IEEE802.2 encapsulation format (DSAP other than 0xAA) is used.
<b>Length</b>	2+1 octets
<b>Value</b>	The octet represents the DSAP which SHALL match with the target.

#### 5.4.2.87 ETH VLAN ID



TLV ID	TLV Name	Length Octets	Occurrence
1	S-VID	2+4	0-1[a]
2	C-VID	2+4	0-1[a]

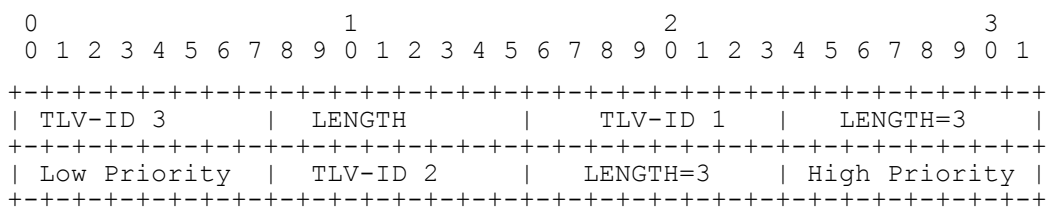
Notes:

[a] At least one value MUST be present.

<b>TLV ID</b>	1 for S-VID
<b>Description</b>	If present, this field specifies the matching value for the IEEE 802.1ad S-VLAN-ID bits. If omitted, the S-VLAN-ID bits are irrelevant for this entry. The field consists of two values, the VID-start and the VID-end, matching all values [VID-start, VID+end]
<b>Length</b>	2+4 octets
<b>Value</b>	Only the lower 12 bits of the 2 byte value are significant; the upper four bits SHALL be ignored.

<b>TLV ID</b>	2 for C-VID
<b>Description</b>	If present, this field specifies the matching value for the IEEE802.1ad C-VLAN-ID bits, if IEEE802.1ad is applied, or the matching value for the IEEE 802.1Q VLAN-ID bits, if IEEE802.1Q is applied. If omitted, the VLAN-ID bits are irrelevant for this entry. The field consists of two values, the VID-start and the VID-end, matching all values [VID-start, VID+end]
<b>Length</b>	2+4 octets
<b>Value</b>	Only the lower 12 bits of the 2 byte value are significant; the upper four bits SHALL be ignored.

#### 5.4.2.88 ETH Priority Range



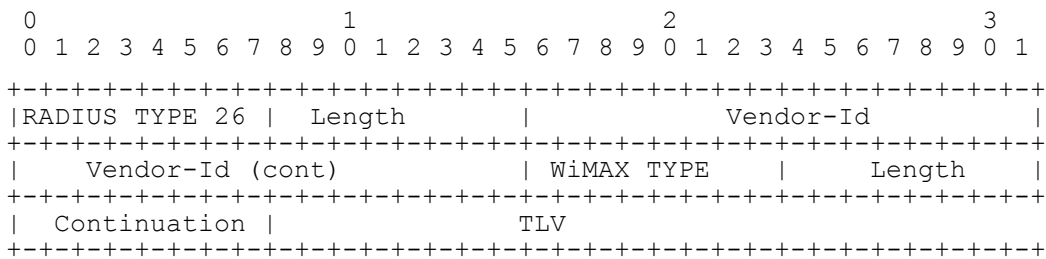
TLV ID	TLV Name	Length Octets	Occurrence
1	ETH Low Priority	2+1	0-1
2	ETH High Priority	2+1	0-1



<b>TLV ID</b>	1 for ETH Low Priority
<b>Description</b>	Lowest priority as specified in IEEE802.1D where a packet SHALL match to.
<b>Length</b>	2+1 octets
<b>Value</b>	Priority as specified in IEEE802.1D with a valid range from 0 to 7.

<b>TLV ID</b>	2 for ETH High Priority
<b>Description</b>	Highest priority as specified in IEEE802.1D where a packet SHALL match to.
<b>Length</b>	2+1 octets
<b>Value</b>	Priority as specified in IEEE802.1D with a valid range from 0 to 7.

#### 5.4.2.89 VLANTagProcessing Descriptor



<b>Type-ID</b>	85 for VLANTagProcessing Descriptor
<b>Description</b>	This attribute describes the rules for the processing of the VLAN tags of an ETH packet flow. The VLANTagProcessing descriptor may be pre-provisioned.
<b>Length</b>	6 + 3 + TLVs
<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	VLANTagProcessingRuleID	2+2	0	1[a]	0	0
2	C-VLAN Priority Setting	2+1	0	1[b]	0	0
3	VLAN ID Assignment	2+2	0	0-1	0	0
4	C-VLAN ID	2+2	0	0-1	0	0
5	S-VLAN ID	2+2	0	0-1	0	0
6	C-VID>S-VID Mapping	2+4	0	0-n	0	0
7	LocalConfigInfo[c]	2+n	0	0-1	0	0

Notes:

- [a] VLANTagProcessingRuleID = 0 is reserved with special meaning that no VLANTagProcessing is performed for the particular service flow regardless of any preprovisioned rule.
- [b] C-VLAN Priority Setting is always present
- [c] LocalConfigInfo is an arbitrary information element provided by the CSN in the case of preprovisioned R3 data path (Simple Ethernet), which may be used for local configuration purposes. LocalConfigInfo is not used in the case of MIP based R3 data path.

1

<b>TLD ID</b>	1 for VLANTagProcessingRuleID
<b>Description</b>	ID of the particular rule
<b>Length</b>	2+2
<b>Value</b>	Unsigned-Short <ul style="list-style-type: none"> <li>• 0x0000: reserved with special meaning</li> </ul>

2

<b>TLD ID</b>	2 for C-VLAN Priority Setting
<b>Description</b>	Defines the setting of the priority_bits in the C-VLAN tag in the upstream direction.
<b>Length</b>	2+1
<b>Value</b>	Bitfield; the bits have the following meaning: <ul style="list-style-type: none"> <li>• 0x00 = forward the p_bits without modification</li> <li>• 0x1x = drop frames with p_bits set to a higher value than x</li> <li>• 0x2x = set p_bits to x when p_bits set to a higher value than x</li> <li>• 0x3x = set the p_bits to x: insert VLAN tag with VLAN-ID=0 and p_bits set to value x into Ethernet frames without VLAN tag.</li> </ul> Other values reserved. Note: One of the bitfield definitions can be assigned at a time.

3

<b>TLD ID</b>	3 for VLAN ID Assignment
<b>Length</b>	2+2
<b>Description</b>	Defines the processing of the C-VLAN tag and S-VLAN tag

<b>Value</b>	<p>Bitfield; the bits have the following meaning:</p> <ul style="list-style-type: none"> <li>0x0000 = forward VLAN tags without modification</li> <li>0x0010 = remove S-VID in downstream direction</li> <li>0x0020 = remove C-VID and S-VID, if present, in downstream direction</li> <li>0x010x = add C-VLAN tag in upstream to frames without C-VLAN tag with C-VID set to C-VLAN ID and p_bits set to x</li> <li>0x020x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set to S-VLAN ID and S-p_bits set to x</li> <li>0x0280 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set to S-VLAN ID and S-p_bits copied from C-p_bits</li> <li>0x040x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C-&gt;S-VID Mapping table and S-p_bits set to x If no entry exists for a particular C-VID in the C-&gt;S-VID Mapping table, the S-VID is set to 0</li> <li>0x0480 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C-&gt;S-VID Mapping Table and S-p_bits copied from C-p_bits If no entry exists for a particular C-VID in the C-&gt;S-VID Mapping table, the S-VID is set to 0</li> </ul> <p>Other values reserved. One downstream rule can be combined (ORed) with one upstream rule.</p>
--------------	---

1

<b>TLV ID</b>	4 for SVLAN-ID
<b>Description</b>	The value of the field specifies the SVALN ID value for the Ethernet frame.
<b>Length</b>	2+2
<b>Value</b>	Only the lower 12 bits of the 2 byte value are significant; the upper four bits SHALL be ignored.

2

<b>TLV ID</b>	5 for CVLAN-ID
<b>Description</b>	The value of the field specifies the CVLAN-ID value for the Ethernet frame.
<b>Length</b>	2+2
<b>Value</b>	Only the lower 12 bits of the 2 byte value are significant; the upper four bits SHALL be ignored.

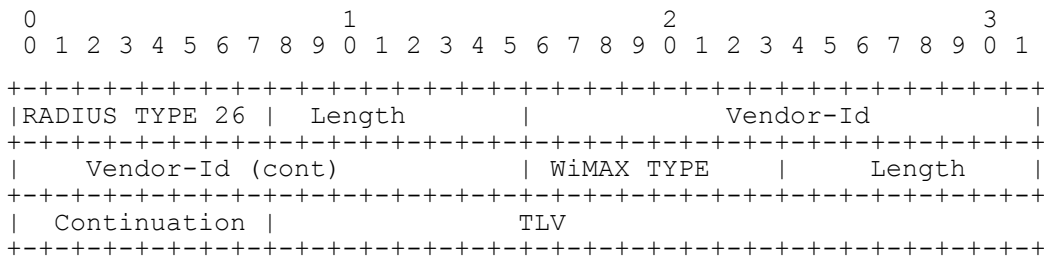
3

<b>TLV ID</b>	6 for C-VID>S-VID Mapping
<b>Description</b>	The value of the field specifies a mapping between a C-VID and a S-VID
<b>Length</b>	2+4
<b>Value</b>	<p>C-VID,S-VID</p> <p>Only the lower 12 bits of the 2 byte VID values are significant; the upper four bits SHALL be ignored.</p>

4

<b>TLD ID</b>	7 for LocalConfigInfo
<b>Description</b>	Local configuration information for preprovisioned R3 data path (Simple Ethernet)
<b>Length</b>	2+n
<b>Value</b>	String of length n containing arbitrary information The meaning of the information in LocalConfigInfo is subject of static configuration agreements between NAP and NSP.

#### 5.4.2.90 hDHCP-Server-Parameters



<b>WType-ID</b>	86 for hDHCP-Server-Parameters
<b>Description</b>	This attribute contains the Home DHCP server and corresponding security keys.
<b>Length</b>	6 + 3 + TLVs
<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	DHCPv4-Server	2+4	0	0-1[a]	0	0
2	DHCPv6-Server	2+16	0	0-1 [a]	0	0
3	DHCP-RK	2+2+Length	0	0-1[b]	0	0
4	DHCP-RK-ID	2+4	0	0-1[b]	0	0
5	DHCP-RK-Lifetime	2+4	0	0-1[b]	0	0

#### Notes:

- [a] Either DHCPv4-ServerIP-Address or DHCPv6-ServerIP-Address SHALL be present.
- [b] 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.

<b>TLV ID</b>	1 for DHCPv4-Server
<b>Description</b>	The IPv4 address of the home DHCP-Server to use for IPv4 address allocation by the ASN.
<b>Length</b>	2+4
<b>Value</b>	Octet string containing an IPv4 address (most significant bit first).

<b>TLV ID</b>	2 for DHCPv6-Server
<b>Description</b>	The IPv6 address of the home DHCP-Server to use for IPv6 allocation by the ASN.
<b>Length</b>	2+16
<b>Value</b>	Octet string containing an IPv6 address (most significant bit first).

<b>TLV ID</b>	3 for DHCP-RK
<b>Description</b>	The hDHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
<b>Length</b>	2 + 2(SALT) + length of the String containing the encrypted hDHCP-RK.
<b>Value</b>	The value consists of 2 octets for the SALT (see [47]) and a String containing the encrypted hDHCP-RK formulated as per [47].

<b>TLV ID</b>	4 for DHCP-RK-Key-ID
<b>Description</b>	An integer number uniquely identifying the hDHCP-RK within the scope of a single DHCP server.
<b>Length</b>	2 + 4
<b>Value</b>	Unsigned 32-bit integer MSB first.

<b>TLV ID</b>	5 for DHCP-RK-Lifetime
<b>Description</b>	Lifetime of the hDHCP-RK and derived keys.
<b>Length</b>	2 + 4
<b>Value</b>	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

#### 5.4.2.91 vDHCP-Server-Parameters

```

      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
9      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
10     |RADIUS TYPE 26 | Length          | Vendor-Id          |
11     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
12     | Vendor-Id (cont) | WiMAX TYPE    | Length          |
13     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
14     | Continuation | TLV
15     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	87 for vDHCP-Server-Parameters
<b>Description</b>	This attribute contains a Visited DHCPv4 server and corresponding security keys.
<b>Length</b>	6 + 3 + TLVs
<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	DHCPv4-Server	2+4	0-1[c]	0-1[a]	0	0
2	DHCPv6-Server	2+16	0-1[c]	0-1 [a]	0	0
3	DHCP-RK	2+2+Length	0	0-1[b]	0	0
4	DHCP-RK-ID	2+4	0	0-1[b]	0	0
5	DHCP-RK-Lifetime	2+4	0	0-1[b]	0	0

**Notes:**

- [a] Either DHCPv4-ServerIP-Address or DHCPv6-ServerIP-Address SHALL be present.
- [b] 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.
- [c] The visited AAA can include the DHCPv4-Server-Address or DHCPv6-Server-Address to indicate that it is able to assign the DHCP servers for the session.

<b>TLV ID</b>	1 for DHCPv4-Server
<b>Description</b>	The IPv4 address of the visited DHCP-Server to use for IPv4 address allocation by the ASN.
<b>Length</b>	2+4
<b>Value</b>	Octet string containing an IPv4 address (most significant bit first).

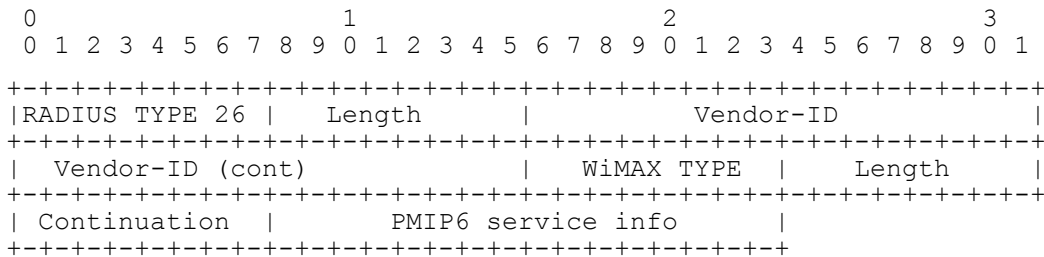
<b>TLV ID</b>	2 for DHCPv6-Server
<b>Description</b>	The IPv6 address of the home DHCP-Server to use for IPv6 allocation by the ASN.
<b>Length</b>	2+16
<b>Value</b>	Octet string containing an IPv6 address (most significant bit first).

<b>TLV ID</b>	3 for DHCP-RK
<b>Description</b>	The DHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
<b>Length</b>	2 + 2(SALT) + length of the String containing the encrypted vDHCP-RK.
<b>Value</b>	The value consists of 2 octets for the SALT (see [47]) and a String containing the encrypted hDHCP-RK formulated as per [47].

<b>TLV ID</b>	4 for DHCP-RK-Key-ID
<b>Description</b>	An integer number uniquely identifying the vDHCP-RK within the scope of a single DHCP server.
<b>Length</b>	2 + 4
<b>Value</b>	Unsigned 32-bit integer MSB first.

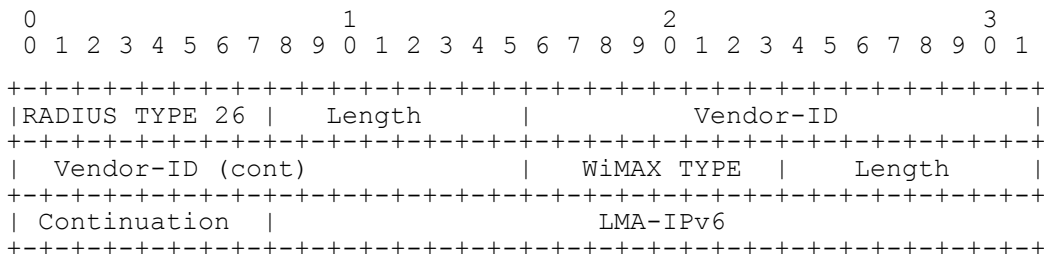
<b>TLV ID</b>	5 for DHCP-RK-Lifetime
<b>Description</b>	Lifetime of the DHCP-RK and derived keys.
<b>Length</b>	2 + 4
<b>Value</b>	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

#### 5.4.2.92 PMIP6-Service-Info



<b>WType-ID</b>	126 for PMIP6-Service-Info
<b>Description</b>	Included in Access-Request this attribute indicates which PMIP6 features are supported and enabled in the ASN/VCSN. When included in Access-Accept this attribute indicates which of the protocol features are authorized for subscriber's IP session and corresponding ASN/VCSN.
<b>Length</b>	6 + 3 + 2
<b>Continuation</b>	C-bit = 0
<b>Value</b>	<p>2 Octets Bitmask defined as follows:</p> <ul style="list-style-type: none"> <li>• Bit #0 = Mobility support for IPv6</li> <li>• Bit #1 = Mobility support for IPv4</li> <li>• Bit #2 = IPv4 transport backhaul support</li> <li>• Bit #3 = Lower-layer transport security</li> <li>• Bit #4 = In-band protocol security</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

#### 5.4.2.93 hLMA-IPv6-PMIP6



<b>WType-ID</b>	127 for hLMA-IPv6-PMIP6
<b>Description</b>	The IPv6 address of the LMA in the HCSN assigned for the MS's PMIP6 session.
<b>Length</b>	6 + 3 + 16

<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet-String representing an IPv6 address (the most significant octet first)

#### 5.4.2.94 hLMA-IPv4-PMIP6

```

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 | LMA-IPv4
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	128 for hLMA-IPv4-PMIP6
<b>Description</b>	The IPv4 address of the LMA in the HCSN assigned for the MS's PMIP6 session.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet-String representing an IPv4 address (the most significant octet first)

#### 5.4.2.95 vLMA-IPv6-PMIP6

```

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 | LMA-IPv6
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	129 for vLMA-IPv6-PMIP6
<b>Description</b>	The IPv6 address of the LMA in the VCSN assigned for the MS's PMIP6 session.
<b>Length</b>	6 + 3 + 16
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet-String representing an IPv6 address (the most significant octet first)

#### 5.4.2.96 vLMA-IPv4-PMIP6

```

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 | LMA-IPv4
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```



<b>WType-ID</b>	130 for vLMA-IPv4-PMIP6
<b>Description</b>	The IPv6 address of the LMA in the HCSN assigned for the MS's PMIP6 session.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet-String representing an IPv4 address (the most significant octet first)

#### 5.4.2.97 PMIP6-RK-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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	131 for PMIP6-RK-KEY
<b>Description</b>	The PMIP6-RK-KEY sent by the RADIUS Server to the ASN and hCSN LMA for PMIP6. It is used to calculate the individual LMA-MAG key being the base for PBU and PBA messages protection through mobility authentication options.
<b>Length</b>	6 + 3 +2(SALT)+ Length of the encrypted PMIP6-RK-KEY
<b>Continuation</b>	C-bit = 0
<b>Value</b>	The value consists of 2 octets for the SALT (see [39]) and a String containing the encrypted PMIP6-RK-KEY formulated as per Section 4.3.1.1.

#### 5.4.2.98 PMIP6-RK-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
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	132 for PMIP6-RK-SPI
<b>Description</b>	The SPI associated with the PMIP6-RK-KEY
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned 32-bit integer, MSB first.

#### 5.4.2.99 Home-HNP-PMIP6

```

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 | Prefix-Length | Home-HNP
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	133 for Home-HNP-PMIP6
<b>Description</b>	The IPv6 Home Network Prefix assigned by the AAA in HCSN to the MS for PMIP6 mobility session.
<b>Length</b>	6 + 3 + 1 + (0-16)
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string contains one byte of “Prefix-Length” and up to 16 bytes of Home Network Prefix

#### 5.4.2.100 Home-Interface-Id-PMIP6

```

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 | Home-Interface-Id
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	134 for Home-Interface-Id-PMIP6
<b>Description</b>	The IPv6 interface Id assigned by the HCSN to be used for PMIP6 address configuration via DHCPv6
<b>Length</b>	6 + 3 + 8
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing the IPv6 interface identifier (most significant bit first)

#### 5.4.2.101 Home-IPv4-HoA-PMIP6

```

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 | Prefix-Length | Home-IPv4-HoA
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	135 for Home-IPv4-HoA-PMIP6
<b>Description</b>	The IPv4 Home Address assigned by the HCSN to the MS for PMIP6-IPv4 mobility

	session.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing the IPv4 address (most significant bit first)

#### 5.4.2.102 Visited-HNP-PMIP6

```

0
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 | Prefix-Length | Visited-HNP
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	136 for Visited-HNP-PMIP6
<b>Description</b>	The IPv6 Home Network Prefix assigned by VCSN to the MS for PMIP6 mobility session.
<b>Length</b>	6 + 3 + 1 + (0-16)
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string contains one byte of “Prefix-Length” and up to 16 bytes of Home Network Prefix

#### 5.4.2.103 Visited-Interface-Id-PMIP6

```

0
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 | Visited-Interface-Id
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	137 for Visited-Interface-Id-PMIP6
<b>Description</b>	The IPv6 interface Id assigned by the VCSN to be used for PMIP6 address configuration via DHCPv6
<b>Length</b>	6 + 3 + 8
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing the IPv6 interface identifier (most significant bit first)

1

2  
3  
4  
5  
6  
7  
8  
9  
10

<b>WType-ID</b>	138 for Visited-IPv4-HoA-PMIP6
<b>Description</b>	The IPv4 Home Address assigned by the VCSN to the MS for PMIP6-IPv4 mobility session.
<b>Length</b>	6 + 3 + 4
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Octet string containing the IPv4 address (most significant bit first)

## 11

12  
13  
14  
15  
16  
17  
18  
19  
20

<b>WType-ID</b>	88 for BS-Location
<b>Description</b>	An alternative Serving BS identification information to BS-ID. Normally indicates the location information of the serving BS which may be described as Lat/Long/Sector/carrier information of the serving BS.
<b>Length</b>	6 + 3 + Length of Location (>0)
<b>Continuation</b>	C-bit = 0 or 1
<b>Value</b>	Octet string representing location. Format is 0.

## 21

22  
23  
24  
25  
26  
27  
28  
29  
30

<b>WType-ID</b>	89 for Mobility-Access-Classifer
<b>Description</b>	In an Access-Accept the attribute identifies the classification of the subscriber at the H-

	AAA as a fixed, nomadic or mobile access subscriber.
<b>Length</b>	6 + 3 + 1
<b>Continuation</b>	C-bit = 0
<b>Value</b>	<ul style="list-style-type: none"> <li>1 = Fixed</li> <li>2 = Nomadic</li> <li>3 = mobile</li> <li>4-255= Reserved</li> </ul>

#### 5.4.2.107 MS-Authenticated

```

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 |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	90 for MS-Authenticated
<b>Description</b>	A flag indicating whether the MS has successfully performed device authentication during initial network entry or not.
<b>Length</b>	6 + 3 + 1
<b>Continuation</b>	C-bit = 0
<b>Value</b>	Unsigned Octet. When set to (1) the MS has successfully performed device authentication during initial network entry as part of which the MAC address has also been authenticated. When set to (0) the MS has not performed device authentication.

#### 5.4.2.108 Operator-Name

```

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 | Length | Vendor-ID |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Text (cont.) |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	To be assigned by IETF for Operator-Name
<b>Description</b>	This attribute is defined in [96] and contains the country code and the WiMAX assigned company code of the role of the WiMAX operator.
<b>Length</b>	62 + 1 + 7
<b>Value</b>	<p>The Text field is formatted as follows:</p> <pre> 0                               1                               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... +---+   Namespace ID   Operator-Name </pre>

1 5.4.2.109Certified-MS-Feature-List-For-GW

11

12

Page - 874  
WiMAX FORUM PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

1

<b>TLV ID</b>	1 for Certified-For-MCBCS
<b>Description</b>	Indicates the MCBCS features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any MCBCS features.
<b>Length</b>	2+1 octet
<b>Value</b>	The following one octet Bit-map represent the MCBCS features that the MS is certified for: <ul style="list-style-type: none"> <li>• Bit-#0 - Certified_for_MCBCS-App</li> <li>• Bit #1 - Certified_for_MCBCS-DSx</li> </ul> All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

2

<b>TLV ID</b>	2 for Certified-For-LBS
<b>Description</b>	Indicates the LBS features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any LBS features
<b>Length</b>	2+1 octet
<b>Value</b>	The following one octet Bit-map represent the LBS features that the MS is certified for: <ul style="list-style-type: none"> <li>• Bit-#0 - Certified_for_LBS-Control-Plane</li> <li>• Bit #1 - Certified_for_LBS-Hybrid</li> </ul> All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

3

<b>TLV ID</b>	3 for Certified-Compression
<b>Description</b>	Indicates the Compression features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any Compression features.
<b>Length</b>	2+1 octet
<b>Value</b>	The following one octet Bit-map represent the Compression features that the MS is certified for: <ul style="list-style-type: none"> <li>• Bit-#0 - Certified_for_ROHC</li> <li>• Bit #1 - Certified_for_PHS</li> </ul> All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

4

#### 5.4.2.110 Certified-MS-Feature-List-For-BS

```

6      0          1          2          3
7      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
8      +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
9      |RADIUS TYPE 26 | Length | Vendor-Id |
10     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
11     | Vendor-Id (cont) | WiMAX TYPE | Length |
12     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
13     | Continuation | TLVs
14     +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

<b>WType-ID</b>	140 for Certified-MS-Feature-List-For-BS
<b>Description</b>	List of MS Certified features relevant for the BS policy for this MS. This acts as a container for the list of allowed certified MS feature for the BS to activate (e.g., MIMO, Hybrid ARQ, etc). Upon receipt the ASN-GW transparently forwards the Certified-MS-Feature-List-For-BS to the BS across R4/R6.
<b>Length</b>	6 + 3 + TLVs
<b>Continuation</b>	C-bit = 0
<b>Value</b>	One or more of the following sub-TLVs

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	Certified-Scan-Capability	3	0	0-1	0	0
2	Certified-Security-Capability	3	0	0-1	0	0
3	Certified-ARQ-Capability	3	0	0-1	0	0

<b>TLV ID</b>	1 for Certified-Scan-Capability
<b>Description</b>	Indicates the Scan Capability features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any Scan Capability features.
<b>Length</b>	2+1 octet
<b>Value</b>	<p>The following one octet Bit-map represent the Scan Capability features that the MS is certified for:</p> <ul style="list-style-type: none"> <li>• Bit-#0 – Certified for HO Scanning</li> <li>• Bit-#1 – Certified for Scan Report Type Support</li> <li>• Bit-#2 – Certified for HO/Scan/Report Trigger Metrics</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

<b>TLV ID</b>	2 for Certified-Security-Capability
<b>Description</b>	Indicates the Security Capability features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any Security Capability features.
<b>Length</b>	2+1 octet
<b>Value</b>	<p>The following one octet Bit-map represent the Security Capability features that the MS is certified for:</p> <ul style="list-style-type: none"> <li>• Bit-#0 – Certified for PKM message encoding support</li> <li>• Bit-#1 – Certified for Authorization policy support – Initial Network entry</li> <li>• Bit-#2 – Certified for Authorization policy support – Network re-entry</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>



<b>TLV ID</b>	3 for Certified-ARQ-Capability
<b>Description</b>	Indicates the ARQ Capability features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any ARQ Capability features.
<b>Length</b>	2+1 octet
<b>Value</b>	<p>The following one octet Bit-map represent the ARQ Capability features that the MS is certified for:</p> <ul style="list-style-type: none"> <li>• Bit-#0 – Certified for Sending and Receiving PDU for ARQ</li> <li>• Bit-#1 – Certified for ARQ feedback message</li> <li>• Bit-#2 – Certified for ARQ Discard message</li> <li>• Bit-#3 – Certified for ARQ Reset message</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

## 5.5 Diameter Applications, Commands and AVPs

The section lists the standard attributes that are used across Diameter-based WiMAX reference points, and all VSAs (vendor-specific attributes) that are defined for WiMAX network operation as describe by this specification.

Diameter nodes supporting Network Access Authentication and Authorization conforming to this specification MUST advertise support by including the WiMAX vendor specific Application Identifier listed in the table below in the Auth-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer command RFC3588 [54].

Application ID	Application Name	Description
<IANA Pending>WNAADA	WiMAX Network Access Authentication and Authorization Diameter Application	Application between the ASN and the AAA in the CSN.
<IANA Pending>WNADA	WiMAX Network Accounting Diameter Application	Application between the ASN or HA and the AAA in the CSN
<IANA Pending>WM4DA	WiMAX MIP4 Diameter Application	Application between the MIP4 HA and the AAA in the CSN for IPv4 mobility service.
<IANA Pending>WM6DA	WiMAX MIP6 Diameter Application	Application between the MIP6 HA and the AAA in the CSN.
<IANA Pending>WDDA	WiMAX DHCP Diameter Application	Application between the DHCP Server and the AAA in the CSN.

A WiMAX compliant ASN-GW MUST advertise support for the WiMAX Network Access Authentication and Authorization Diameter Application (<IANA Pending>WNAADA) and WiMAX Network Accounting Diameter Application when performing the Capability Exchange procedure defined in RFC3588 [54].

A WiMAX compliant VAAA MUST advertise support for the WiMAX Network Access Authentication and Authorization Diameter Application (<IANA Pending>WNAADA) when performing the Capability Exchange procedure defined in RFC3588 [54].

A WiMAX compliant HA providing IPv4 mobility services MUST advertise support for the WiMAX MIP4 Diameter Application (<IANA Pending>WM4DA) and MAY advertise WiMAX Network Accounting Diameter Application when performing the Capability Exchange procedure defined in RFC3588 [54].

A WiMAX compliant HA providing IPv6 mobility services MUST advertise support for the WiMAX MIP6 Diameter Application (<IANA Pending>WM6DA) and MAY advertise WiMAX Network Accounting Diameter Application when performing the Capability Exchange procedure defined in RFC3588 [54].

A WiMAX compliant DHCP server MUST advertise support for the WiMAX DHCP Diameter Application (<IANA Pending>WDDA) when performing the Capability Exchange procedure defined in RFC3588 [54].

A WiMAX compliant HAAA MUST advertise support for the WiMAX Network Access Authentication and Authorization Diameter Application (<IANA Pending>WNAADA), WiMAX MIP4 Diameter Application and WiMAX Network Accounting Diameter Application when performing the Capability Exchange procedure defined in RFC3588 [54]. The HAAA MAY advertise support for WiMAX MIP6 Diameter Application and WiMAX DHCP Diameter Application when performing the Capability exchange procedure defined in RFC3588 [54].

## 5.5.1 Diameter Applications and Messages

### 5.5.1.1 WiMAX Network Access Authentication and Authorization Diameter Application

The WiMAX Network Access Authentication and Authorization Diameter Application is based on the Diameter Extensible Authentication Protocol (EAP) Application as specified in RFC4072 [66]. New WiMAX versions of the commands have been created to reflect modifications to the ABNF. Two new commands WCAR and WCAA are defined to support change of authorization. The following table lists all of the commands that are applicable to the WiMAX Network Access Authentication and Authorization Diameter Application:

**Table 5-16 – Commands of WiMAX Network Access Authentication and Authorization Diameter Application**

Command-Name	Abbrev.	Code
WiMAX-Diameter-EAP-Request	WDER	<IANA Pending>WDE
WiMAX-Diameter-EAP-Answer	WDEA	<IANA Pending>WDE
WiMAX-Change-of-Authorization-Request	WCAR	<IANA Pending>WCA
WiMAX-Change-of-Authorization-Answer	WCAA	<IANA Pending>WCA
WiMAX-Reauthentication-Request	WRAR	<IANA Pending>WRA
WiMAX-Reauthentication-Answer	WRAA	<IANA Pending>WRA
WiMAX-Session-Termination-Request	WSTR	<IANA Pending>WST
WiMAX-Session-Termination-Answer	WSTA	<IANA Pending>WST
WiMAX-Abort-Session-Request	WASR	<IANA Pending>WAS
WiMAX-Abort-Session-Answer	WASA	<IANA Pending>WAS

#### 5.5.1.1.1 WiMAX Diameter-EAP-Request/Answer Commands

The following describes only the WiMAX specific VSA that are being added to the WDER and WDEA commands.

## WiMAX Diameter-EAP-Request (WDER) Command

The WiMAX Diameter EAP-Request Command is derived from the DER Command as specified for the Diameter EAP Application in RFC 4072 [66] and is used to carry out EAP authentication between the ASN and the CSN.

The WiMAX Network Access and Authorization Diameter Application extends the DER command by adding the following WiMAX AVPs:

<WiMAX Diameter-EAP-Request> ::= < Diameter Header: TBDWDE , REQ, PXY >

\* \* \* \* \*

Attributes defined in RFC4072.

[ Calling-Station-Id ]

In WiMAX, the Calling Station-Id is set to the MAC address of the device as a 17 byte Upper Case ASCII value as defined by RFC 3580 sec 3.21 and 802-2001 in canonical order. For example "00-10-A4-23-19-C0" is Valid and 00-10-a4-23-19-c0 is not valid; and 00:10:A4:23:19:C0 is not valid.

[ Chargeable-User-Identity ]

[ WiMAX-Capability ]

[ WiMAX-Session-Id ]

[GMT-Time-Zone-Offset]

[BS-ID]

[NAP-ID]

[NSP-ID]

[ Operator-Name ]

The WiMAX WRI-Code of the VN-SP.

### Support for Mobility Services

[vHA-IP-MIP4]

[vHA-IP-MIP6]

[Visited-Framed-IP-Address]

[Visited-Framed-IPv6-Prefix]

[Visited-Framed-Interface-Id]

### Support for DHCP Relay Service

[vDHCPv4-Server]

The VCSN MAY include the vDHCPv4-Server to indicate that it is capable of assigning an IPv4 DHCP server for the session. If the VCSN includes DHCPv4-Server attribute then it SHALL also include the vHA-IP-MIP4 attribute. If VCSN is

capable of assigning more than one IPv4 DHCP server the first one will be present in vDHCPv4-Server attribute and the rest will be present in vDHCP-Server-Parameters.

[vDHCPv6-Server]

The VCSN MAY include the vDHCPv6-Server to indicate that it is capable of assigning an IPv6 DHCP server for the session. If the VCSN includes vDHCPv6-Server then it SHALL also include the vHA-IP-MIP6 attribute. If VCSN is capable of assigning more than one IPv6 DHCP server the first one will be present in vDHCPv6-Server attribute and the rest will be present in vDHCP-Server-Parameters.

[vDHCP-Server-Parameters]

If more than one vDHCP-Server (IPv4 or IPv6 DHCP server) is sent then the first one will be present in vDHCPv4-Server or vDHCPv6-Server attribute and the rest will be present in vDHCPv4-Server-Parameters attribute.

Fixed Nomadic

[BS-Location]

Future Extensibility

\* [ AVP ]

- 1
- 2 Table of occurrence of WiMAX VSAs in a DER command for initial authentication, that is, a DER command that
- 3 has Auth-Request-Type set to AUTHORIZE\_AUTHENTICATE and containing EAP Response(Identity).

4 **Table 5-17 – WDER command in case of initial authentication**

Attribute	Occurrence	Notes
WiMAX-Capability	1	
WiMAX-Session-Id	0-1	MUST be included if the Diameter client received the WiMAX-Session-Id for this mobile. Otherwise it MUST not be included.
Calling-Station-Id	1	SHALL be included in the initial authentication.
GMT-Time-Zone-Offset	1	MUST be included.
BS-ID	0-1	Either the BS-ID or the NAP-ID MUST be included. If both are provided then the receiver SHALL ignore the NAP-ID attribute.

NAP-ID	0-1	Either the BS-ID or the NAP-ID MUST be included. If both are provided then the receiver SHALL ignore the NAP-ID attribute.
NSP-ID	0-1	SHALL be present when the DER command arrives at the HAAA. Either the NAS (if it knows it) or the VCSN SHALL insert this attribute in the DER.
Operator-Name	0-1	SHALL NOT be added to the WDER by the NAS. If added, it SHALL be added by the VNSP.
Visited-Framed-IP-Address	0-1	This Attribute is present between VAAA and HAAA only when VAAA wants to propose IPv4 address in DER.  If this attribute is included then the vHA-IP-MIP4 address MUST also be included.
Visited-Framed-IPv6-Prefix	0-1	This Attribute is present between VAAA and HAAA only when VAAA wants to propose IPv6 address in DER.  If this attribute is included then the vHA-IP-MIP6 address MUST also be included.
Visited-Framed-Interface-Id	0-1	This Attribute is present between VAAA and HAAA only when VAAA wants to propose IPv6 address in DER.  If this attribute is included then Visited-Framed-IPv6-Prefix MUST also be included.
vHA-IP-MIP4	0-1	The ASN or proxy AAA/v-AAA MAY include the vHA-IP-MIP4 AVP set to the IPv4 address of the HA which it proposes to be used for MIP4 services for the session.
vHA-IP-MIP6	0-1	The ASN or proxy AAA/v-AAA MAY include the vHA-IP-MIP6 AVP set to the IPv6 address of the HA which it proposes to be used for MIP6 services for the session.
vDHCPv4-Server	0-1	The VCSN MAY include the vDHCPv4-Server to indicate that it is capable of assigning an IPv4 DHCP server for the session. If the VCSN includes DHCPv4-Server attribute then it SHALL also include the vHA-IP-MIP4 attribute.
vDHCPv6-Server	0-1	The VCSN MAY include the vDHCPv6-Server to indicate that it is capable of assigning an IPv6 DHCP server for the session. If the VCSN includes vDHCPv6-Server then it SHALL also include the vHA-IP-MIP6 attribute.
vDHCP-Server-Parameters	0-n	The VCSN MAY include vDHCP-Server-Parameters if it is capable of assigning more than one IPv4 or IPv6 DHCP server.
BS-Location	0-1	May be used as an alternative Serving BS identifier and usually indicates the location information of the BS which may be described as Lat/Long/Sector/Carrier information of the serving BS.

1  
2

Table of occurrence of WiMAX VSAs in a DER command which is sent in response to a DEA command with Result-Code=DIAMETER\_MULTI\_ROUND\_AUTH. This is equivalent to a RADIUS request which is sent in response to a RADIUS Access-Challenge message. The sole purpose of these exchanges is to progress the EAP authentication method. Thus, only, EAP AVP and session identification AVP must be carried as described below.

**Table 5-18 – WDER command when sent in response to DEA with Result-Code  
DIAMETER\_MULTI\_ROUND\_AUTH**

Attribute	Occurrence	Notes
WiMAX-Capability	0-1	MAY contain the WiMAX-Capability. Unless otherwise allowed, attributes contained within the WiMAX-Capability MUST remain the same as originally sent in the initial DER command.
Calling-Station-Id	0-1	MAY be included but SHALL match the value sent in the initial authentication.
WiMAX-Session-Id	1	As received in the DEA.
GMT-Time-Zone-Offset	0-1	If included MUST be the same as sent in the initial DER.
BS-ID	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
NAP-ID	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
NSP-ID	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
Operator-Name	0-1	If included MUST only be included by the VNSP and it MUST be the same value as sent in the DER containing the EAP-Response Identity.
Visited-Framed-IP-Address	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
Visited-Framed-IPv6-Prefix	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
Visited-Framed-Interface-Id	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
vHA-IP-MIP4	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
vHA-IP-MIP6	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
vDHCPv4-Server	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity.
vDHCPv6-Server	0-1	If included MUST be the same as sent in the DER containing the EAP-Response Identity
vDHCP-Server-Parameters	0-n	If included MUST be the same as sent in the DER containing the EAP-Response Identity

Table of occurrence of WiMAX VSAs in a DER command which is sent in the case of re-authentication. The Auth-Request-Type SHALL be set to AUTHENTICATE\_ONLY.

1

**Table 5-19 – WDER command when Request-Type is AUTHENTICATE\_ONLY**

Attribute	Occurrence	Notes
WiMAX-Capability	1	Unless otherwise allowed, attributes contained within the WiMAX-Capability MUST remain the same as originally sent in the initial DER command.
WiMAX-Session-Id	1	As received in the DEA during initial authentication.
GMT-Time-Zone-Offset	1	MUST be included.
BS-ID	0-1	Either the BS-ID or the NAP-ID MUST be included. If both are provided then the receiver SHALL ignore the NAP-ID attribute.
NAP-ID	0-1	Either the BS-ID or the NAP-ID MUST be included. If both are provided then the receiver SHALL ignore the NAP-ID attribute.
NSP-ID	0-1	SHALL be present when the DER command arrives at the HAAA. Either the NAS (if it knows it) or the VCSN SHALL insert this attribute in the DER.
Operator-Name	0-1	SHALL NOT be added to the WDER by the NAS. If added, it SHALL be added by the VNSP.
Visited-Framed-IP-Address	0-1	SHOULD NOT be included. But if included it should be the same value as sent in the initial DER. The receiver MUST ignore this value.
Visited-Framed-IPv6-Prefix	0-1	SHOULD NOT be included. But if included it should be the same value as sent in the initial DER. The receiver MUST ignore this value.
Visited-Framed-Interface-Id	0-1	SHOULD NOT be included. But if included it should be the same value as sent in the initial DER. The receiver MUST ignore this value.
vHA-IP-MIP4	0-1	SHOULD NOT be included. But if included it should be the same value as sent in the initial DER. The receiver MUST ignore this value.
vHA-IP-MIP6	0-1	SHOULD NOT be included. But if included it should be the same value as sent in the initial DER. The receiver MUST ignore this value.
vDHCPv4-Server	0-1	SHOULD NOT be included. But if included it should be the same value as sent in the initial DER. The receiver MUST ignore this value.
vDHCPv6-Server	0-1	SHOULD NOT be included. But if included it should be the same value as sent in the initial DER. The receiver MUST ignore this value.
vDHCP-Server-Parameters	0-n	SHOULD NOT be included. But if included it should be the same value as sent in the initial DER. The receiver MUST ignore this value.

2

3 Table of WiMAX attribute for the DER Command.

**Table 5-20 – Attributes of the WDER command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must Not
WiMAX-Capability	1	Grouped		M,V	
Chargeable-User-Identity	89	OctetString	RFC4372 [74]		V
Calling-Station-Id	31	UTF8String	RFC4005 [62]	M	V
Operator-Name	235	UTF8String	[96]	M	V
WiMAX-Session-Id	4	OctetString		M,V	
GMT-Time-Zone-Offset	3	Unsigned32		M,V	
BS-ID	46	OctetString		M,V	
NAP-ID	45	OctetString		M,V	
NSP-ID	57	OctetString		M,V	
Visited-Framed-IP-Address	79	Address		M,V	
Visited-Framed-IPv6-Prefix	80	Address		M,V	
Visited-Framed-Interface-Id	81	OctetString		M,V	
vHA-IP-MIP4	64	Address		M,V	
vHA-IP-MIP6	65	Address		M,V	
vDHCPv4-Server	73	Address		M,V	
vDHCPv6-Server	74	Address		M,V	
vDHCP-Server-Parameters	87	Grouped		M,V	
BS-Location	88	UTF8String		M,V	

Note: M stands for Mandatory to understand attribute by the receiver of the message; and V for Vendor Specific.

#### **WiMAX Diameter-EAP-Answer (WDEA) Command**

The WiMAX Diameter EAP-Answer Command is derived from the DEA Command as specified for the Diameter EAP Application in RFC 4072 [66] and is used to carry out EAP authentication between the ASN and the CSN.

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

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



- 1 The WiMAX Network Access and Authorization Diameter Application extends the DEA command by adding the
- 2 following WiMAX AVPs:

3

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

\* \* \* \* \*

[ WiMAX-Capability ]

[WiMAX-Session-Id ]

\* [Packet-Flow-Descriptor] <sup>34</sup>

\* [Packet-Flow-Descriptor-V2 ]

[QoS-Descriptor]

\* [VLANTagProcessing-Descriptor]

\* [DNS]

[ Operator-Name ]

Contains the WRI-Code of the HNSP.

[MS-Authenticated]

#### Proxy and Client MIP Support

[PMIP-Authenticated-Network-  
Identity]

[Visited-Framed-IP-Address]

[Visited-Framed-IPv6-Prefix]

[Visited-Framed-Interface-Id]

[ hHA-IP-MIP4 ]

[vHA-IP-MIP4]

[hHA-IP-MIP6]

[vHA-IP-MIP6]

[MN-HA-MIP4-MSA]

[MN-vHA-MIP4-MSA]

[FA-RK-MSA]

[HA-RK-MSA]

[vHA-RK-MSA]

#### DHCP Relay Support

[hDHCPv4-Server]

---

<sup>34</sup> This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 SHALL be used in this Release

[vDHCPv4-Server]	.
[hDHCPv6-Server]	
[vDHCPv6-Server]	
[hDHCP-Server-Parameters]	
[vDHCP-Server-Parameters]	
[DHCP-RK-SA]	Conveys the security association to be used when communication with an IPv4 DHCP server allocated in the home network identified by hDHCPv4-Server.
[vDHCP-RK-SA]	Conveys the security association to be used when communication with an IPv4 DHCP server allocated in the visited network identified by vDHCPv4-Server.
[DHCPv6-RK-SA]	Conveys the security association to be used when communication with an IPv6 DHCP server allocated in the home network identified by hDHCPv6-Server.
[vDHCPv6-RK-SA]	Conveys the security association to be used when communication with an IPv6 DHCP server allocated in the visited network identified by vDHCPv6-Server.

#### Hot-Lining Services

[Hotline-Profile-ID]  
[HTTP-Redirection-Rule]  
[IP-Redirection-Rule]  
[NAS-Filter-Rule]  
[Hotline-Session-Timer]  
[Hotline-Indication]

#### Accounting

\* [Time-Of-Day-Time]

#### Mobility Restriction Support

[Mobility-Access-Classfier]

#### Feature Information

[Certified-MS-Feature-List-For-GW]

[Certified-MS-Feature-List-For-BS]

\* [ AVP ]

- 1
- 2 The following table specifies the rules for including WiMAX VSAs in a DEA command when the Result-Code is
- 3 set to DIAMETER\_MULTI\_ROUND\_AUTH. This is equivalent to the RADIUS Access-Challenge packet.

4 **Table 5-21 – WDEA command when Result-Code is DIAMETER\_MULTI\_ROUND\_AUTH**

Attribute	Occurrence	Notes
WiMAX-Capability	0	
WiMAX-Session-Id	0-1	The Home AAA MAY include the WiMAX-Session-Id.
Packet-Flow-Descriptor	0	This TLV is deprecated in this release and SHALL not be used. Only Packet-Flow-Descriptor-V2 SHALL be used in this Release
Packet-Flow-Descriptor-V2	0	
QoS-Descriptor	0	
VLANTagProcessing-Descriptor	0	
DNS	0	
Operator-Name	0	

#### Proxy and Client MIP Support

PMIP-Authenticated-Network-Identity	0	
Visited-Framed-IP-Address	0	
Visited-Framed-IPv6-Prefix	0	
Visited-Framed-Interface-Id	0	
hHA-IP-MIP4	0	
vHA-IP-MIP4	0	
hHA-IP-MIP6	0	
vHA-IP-MIP6	0	
MN-HA-MIP4-MSA	0	
MN-vHA-MIP4-MSA	0	
MN-HA-MIP6-MSA	0	
MN-vHA-MIP6-MSA	0	
FA-RK-MSA	0	
HA-RK-MSA	0	

vHA-RK-MSA	0	
------------	---	--

#### DHCP Relay Support

hDHCPv4-Server	0	
vDHCPv4-Server	0	
hDHCPv6-Server	0	
vDHCPv6-Server	0	
DHCP-RK-SA	0	
vDHCP-RK-SA	0	
DHCPv6-RK-SA	0	
vDHCPv6-RK-SA	0	
vDHCP-Server-Parameters	0	

#### Hot-Lining Services

Hotline-Profile-ID	0	
HTTP-Redirection-Rule	0	
IP-Redirection-Rule	0	
NAS-Filter-Rule	0	
Hotline-Session-Timer	0	
Hotline-Indication	0	

#### Accounting

Time-Of-Day-Time	0	
------------------	---	--

#### Mobility Restriction Support

Mobility Access-Classifer	0	Indicates the classification of the subscriber at the H-AAA as a fixed, nomadic or mobile access subscriber.
---------------------------	---	--

#### Feature Information

Certified-MS-Feature-List-For-GW	0	
Certified-MS-Feature-List-For-BS	0	

The following table specifies the rules for including WiMAX VSA in a DEA command when the Result-Code is set to DIAMETER\_SUCCESS. This is equivalent to the RADIUS Access-Accept packet.

**Table 5-22 – WDEA command when Result-Code is DIAMETER\_SUCCESS**

Attribute	Occurrence	Notes
WiMAX-Capability	1	
WiMAX-Session-Id	1	.
Packet-Flow-Descriptor	0-n	This TLV is deprecated in this release and SHALL not be used. Only Packet-Flow-Descriptor-V2 SHALL be used in this Release.
Packet-Flow-Descriptor-V2	0-n	
QoS-Descriptor	0-n	MAY be included as described by the Packet-Flow-Descriptor-V2.
VLANTagProcessing-Descriptor	0-n	Conditional mandatory: see requirements for Packet-Flow-Descriptor-V2.
DNS	1-n	MUST be included in the success message, if more than one is given, then the first occurrence is the primary and the rest is secondary.
Operator-Name	0-1	MUST be included by the HAAA if the WDER command contained the Operator-Name attribute.
MS-Authenticated	0-1	SHOULD be included to indicate whether the MS has successfully performed device authentication during initial network entry or not.

#### Proxy and Client MIP Support

PMIP-Authenticated-Network-Identity	0-1	MAY be included if the Home Network wants to assign the NAI used in Proxy Mobile IPv4.
Visited-Framed-IP-Address	0-1	<p>If the attribute was received by the HAAA in a DER and the HAAA allows the Visited network to assign IP address, it echoes back the IP address in DEA to VAAA, and VAAA forwards it to the NAS. If IP address assignment by Visited network is not allowed the HAAA SHALL NOT echo this attribute and the HAAA SHALL send Framed-IP-Address.</p> <p>If the Framed-IP-address from both VCSN and HCSN is available, then an anchor selection mechanism needs to be executed to select the anchor CSN for the data path. The details of this mechanism are outside the scope of this specification.</p> <p>If this attribute is included then a vHA-IP-MIP4 AVP set to an address of an HA that can support the IP address, MUST also be included.</p>

Visited-Framed-IPv6-Prefix	0-1	<p>If the attribute was received by the HAAA in a DER and the HAAA allows Visited network to assign IPv6 address, it echoes back the IPv6 prefix in DEA to VAAA, and VAAA forwards it to the NAS. If IPv6 address assignment by Visited network is not allowed the HAAA SHALL NOT echo this attribute.</p> <p>If the IPv6 address from both VCSN and HCSN is available, then an anchor selection mechanism needs to be executed to select the anchor CSN for the data path. The details of this mechanism are outside the scope of this specification.</p> <p>If this attribute is included then an vHA-IP-MIP6 AVP set to an address of an HA that can support the IPv6 address, MUST also be included</p>
Visited-Framed-Interface-Id	0-1	<p>If the attribute was received by the HAAA in a DER and the HAAA allows Visited network to assign IPv6 address, it echoes back the Interface ID in DEA to VAAA, and VAAA forwards it to the NAS. If IPv6 address assignment by Visited network is not allowed the HAAA SHALL NOT echo this attribute.</p> <p>If the IPv6 address from both VCSN and HCSN is available, then an anchor selection mechanism needs to be executed to select the anchor CSN for the data path. The details of this mechanism are outside the scope of this specification.</p> <p>If this attribute is included then a vHA-IP-MIP6 AVP set to an address of an HA that can support the IPv6 address, MUST also be included.</p> <p>If this attribute is included then Visite-Framed-IPv6-Prefix AVP MUST also be included.</p>
hHA-IP-MIP4	0-1	<p>The Home network MAY include an HA for the session in the home network by sending this parameter.</p> <p>At least hHA-IP-MIP4 or vHA-IP-MIP4 MUST be present in the DEA</p>
vHA-IP-MIP4	0-1	SHALL be included if the Home Network allows the Visited Network to assign an HA to the session.
hHA-IP-MIP6	0-1	<p>SHALL be included if the Home network wants to assign an MIP6 HA in the home network.</p> <p>See vHA-IP-MIP6 note below.</p>
vHA-IP-MIP6	0-1	SHALL be included if the Home network want to allow the Visited network to assign a MIP6 HA. The value is as received in the vHA-IP-MIP6 in the DER command. If both hHA-IP-MIP6 and vHA-IP-MIP6 are included then anchor selection mechanism needs to be executed to select the anchor CSN for the data path. The details of the selection mechanism are outside the scope of this specification.
MN-HA-MIP4-MSA	0-1	MUST be included if PMIP4 is supported
MN-vHA-MIP4-MSA	0-1	MUST be included if PMIP4 is supported to an HA in the visited network. If this attribute is included then vHA-IP-

		MIP4 MUST also be included.
FA-RK-MSA	1	
HA-RK-MSA	0-1	Is included by the HAAA if the hHA-IP-MIP4 attribute is also included in the DEA.
vHA-RK-MSA	0-1	Is included by the VAAA if the vHA-IP-MIP4 attribute is also included in the DEA.  This attribute MUST NOT be included in a DEA by the HAAA.

#### DHCP Relay Support

hDHCPv4-Server	0-1	Is included if the Home Network is assigning an IPv4 DHCP server for the session.
vDHCPv4-Server	0-1	Is included if the Home network is allowing the Visited network to assign an IPv4 DHCP server. The value of this attribute MUST be the same as received in the DEA.
hDHCPv6-Server	0-1	Is included if the Home Network is assigning an IPv6 DHCP server for the session.
vDHCPv6-Server	0-1	Is included if the Home network is allowing the Visited network to assign an IPv6 DHCP server. The value of this attribute MUST be the same as received in the DEA.
DHCP-RK-SA	0-1	MUST be included by the Home AAA if hDCHPv4-Server is included.
vDHCP-RK-SA	0-1	MUST be included by the Visited AAA if vDCHPv4-Server is included. The Home AAA MUST NOT include this attribute.
DHCPv6-RK-SA	0-1	MUST be included by the Home AAA if hDCHPv4-Server is included
vDHCPv6-RK-SA	0-1	MUST be included by the Visited AAA if vDCHPv6-Server is included. The Home AAA MUST NOT include this attribute
hDHCP-Server-Parameters	0-n	Is included if the Home Network is capable of assigning an IPv4 or IPv6 DHCP server for the session.
vDHCP-Server-Parameters	0-n	Is included if the Home network is allowing the Visited network to assign multiple DHCP servers. The value of this attribute MUST be the same as received in the DEA.

#### Hot-Lining Services

Hotline-Profile-ID	0-1	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.
HTTP-Redirection-Rule	0-n	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.
IP-Redirection-Rule	0-n	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.
NAS-Filter-Rule	0-n	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.
Hotline-Session-Timer	0-1	
Hotline-Indication	0-1	If the session is to be Hot-Lined then this attribute SHALL be specified and the NAS SHALL include this attribute in the accounting messages.

#### Accounting

Time-Of-Day-Time	0-n	
------------------	-----	--

#### Feature Information

Certified-MS-Feature-List-For-GW	0	SHALL be present if CRN is received as part of NAI decoration.
Certified-MS-Feature-List-For-BS	0	SHALL be present if CRN is received as part of NAI decoration.

The following attributes are defined in various RFCs and have WiMAX specific consideration as follows:

**Chargeable-User-Identity** As per RFC 4372 [74], in a DER, Chargeable-User-Identity MAY be included if the ASN, VAAA, or other broker AAA want the home network to assign a Chargeable-User-Identity for this session. In this case the HAAA MUST include the Chargeable-User-Identity in DEA messages as follows:

- It MUST be included in a DEA message with a Result-Code of DIAMETER Success.
- It MAY be included in DEA message with Result-Code DIAMETER\_MULTI\_ROUND\_AUTH.

A WiMAX AAA server MAY include the Chargeable-User-Identity attribute in a DEA message irrespective of whether the Chargeable-User-Identity was requested by entities outside the home network (in DER messages).

**Authorization-Lifetime and Session-Timeout** Authorization-Lifetime should be included to specify how long the session should live before re-authenticating (as per RFC 3588 [54]). Session-Timeout,



if included SHALL be set to the same value of Authorization-Lifetime.

If translating to RADIUS, the Authorization-Lifetime is coded as Session-Timeout with Termination Action set to RADIUS.

Filter-Id If the WiMAX Hot-Lining AVP are used then Filter-Id MUST NOT be used.

Framed-IP-Address If this attribute is present then this is the Home Address that SHALL be assigned to the mobile. If this attribute is absent then the Home Address is derived from MIP procedures or other means (E.g. DHCP).

Framed-MTU If the Framed MTU appears in a DER during Access-Authentication then it indicates the MTU on the link between the NAS and the MS. As per [52] the Diameter Server 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.

NAS-Filter-Rule MUST NOT be used if WiMAX Hot-Lining VSA are used for the session.

1

2

**Table 5-23 – Attributes of the WDEA command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must Not
WiMAX-Capability	1	Grouped		M,V	
WiMAX-Session-Id	4	OctetString		M,V	
Chargeable-User-Identity	89	OctetString	RFC4372 [74]		V
Operator-Name	TBD	UTF8String	[96]	M	V
Packet-Flow-Descriptor (This TLV is deprecated in this release)	28	Grouped			
Packet-Flow-Descriptor-V2	84	Grouped		M,V	
QoS-Descriptor	29	Grouped		M,V	
VLANTagProcessing-Descriptor	211	Grouped		M,V	
DNS	52	Address		M,V	
MS-Authenticated	90	Enumerated		M,V	
PMIP-Authenticated-Network-Identity	78	UTF8String		M,V	
Visited-Framed-IP-Address	79	Address		M,V	
hHA-IP-MIP4	6	Address		M,V	
vHA-IP-MIP4	64	Address		M,V	
hHA-IP-MIP6	7	Address		M,V	
vHA-IP-MIP6	65	Address		M,V	

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must Not
MN-HA-MIP4-MSA	328	Grouped		M,V	
MN-vHA-MIP4-MSA	329	Grouped		M,V	
FA-RK-MSA	330	Grouped		M,V	
HA-RK-MSA	331	Grouped		M,V	
vHA-RK-MSA	332	Grouped		M,V	
hDHCPv4-Server	8	Address		M,V	
vDHCPv4-Server	73	Address		M,V	
hDHCPv6-Server	9	Address		M,V	
vDHCPv6-Server	74	Address		M,V	
DHCP-RK-SA	333	Grouped		M,V	
vDHCP-RK-SA	334	Grouped		M,V	
DHCPv6-RK-SA	342	Grouped		M,V	
vDHCPv6-RK-SA	343	Grouped		M,V	
hDHCP-Server-Parameters	86	Grouped		M,V	
vDHCP-Server-Parameters	87	Grouped		M,V	
Hotline-Profile-ID	53	UTF8String		M,V	
HTTP-Redirection-Rule	54	Grouped		M,V	
IP-Redirection-Rule	55	Grouped		M,V	
Hotline-Session-Timer	56	Unsigned32		M,V	
Hotline-Indication	24	UTF8String		M,V	
Mobility-Access-Classfier	89	Enumerated		M,V	
Certified-MS-Feature-List-For-GW	139	Grouped		M,V	
Certified-MS-Feature-List-For-BS	140	Grouped		M,V	
Certified-For-MCBCS	459	OctetString		M,V	
Certified-For-LBS	460	OctetString		M,V	
Certified-Compression	461	OctetString		M,V	
Certified-Scan-Capability	462	OctetString		M,V	
Certified-Security-Capability	463	OctetString		M,V	
Certified-ARQ-Capability	464	OctetString		M,V	

### 5.5.1.1.2 WiMAX Change-of-Authorization-Request/Answer Command

#### WiMAX Change-of-Authorization-Request Command

The WiMAX Change-of-Authorization-Request (WCAR) command, indicated by the Command-Code field set to TBDWCAR, is sent from the AAA to the NAS or to the HA in order to change the authorization state of a device mid-session. This command may also be used by the AAA when it needs to push any kinds of information to the NAS or to the HA mid-session.

The WCAR message format is defined as follows:

<WCA-Request> ::= < Diameter Header: TBDWCA, REQ, PXY >

```

    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
    { Destination-Realm }
    { Destination-Host }
    { Auth-Application-Id }
    { User-Name }
    { WiMAX-Session-Id }
    [ Origin-State-Id ]
    [ Chargeable-User-Identity ]
    * [ Proxy-Info ]
    * [ Route-Record ]
    * [ NAS-Filter-Rule ]
    * [ Framed-IP-Address ]
    * [ Hotline-Profile-ID ]
    * [ HTTP-Redirection-Rule ]
    * [ IP-Redirection-Rule ]
    [ Hotline-Session-Timer ]
    [ Hotline-Indication ]
    * [ AVP ]

```

**Table 5-24 – Attributes of the WCAR command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
WiMAX-Session-Id	4	OctetString	-	M,V	-
Hotline-Profile-ID	53	UTF8String	-	M,V	-
HTTP-Redirection-Rule	54	Grouped	-	M,V	-

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
IP-Redirection-Rule	55	Grouped	-	M,V	-
Hotline-Session-Timer	56	Unsigned32	-	M,V	-
Hotline-Indication	24	UTF8String	-	M,V	-

1

## 2 WiMAX Change-of-Authorization-Answer Command

3 The WiMAX Change-of-Authorization-Answer (WCAA) command, indicated by the Command-Code field set to  
4 TBDWCAA, is sent from the NAS or the HA to the AAA in order to report the result of the WCAR command.

5 The WCAA message format is defined as follows:

6 <WCA-Answer> ::= < Diameter Header: TBDWCA, PXY >

```

    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { User-Name }
    { WiMAX-Session-Id }
    [ Origin-State-Id ]
    [ Chargeable-User-Identity ]
    [ Error-Message ]
    [ Error-Reporting-Host ]
    * [ Failed-AVP ]
    * [ Redirect-Host ]
    [ Redirect-Host-Usage ]
    [ Redirect-Host-Cache-Time ]
    * [ Proxy-Info ]
    * [ AVP ]

```

7

8

**Table 5-25 – Attributes of the WCAA command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Result-Code	268	Unsigned32	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Chargeable-User-Identity	89	OctetString	RFC4372	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	P,V
Route-Record	282	DiamIdentity	RFC3588	M	P,V
Framed-IP-Address	8	OctetString	RFC4005	M	V
NAS-Filter-Rule	400	IPFilterRule	RFC4005	M	V
Error-Message	281	UTF8String	RFC3588	-	V,M
Error-Reporting-Host	294	DiamIdentity	RFC3588	-	V,M
Failed-AVP	279	Grouped	RFC3588	M	V
Redirect-Host	292	DiamURI	RFC3588	M	V
Redirect-Host-Usage	261	Enumerated	RFC3588	M	V
Redirect-Host-Cache-Time	262	Unsigned32	RFC3588	M	V

#### 5.5.1.1.3 WiMAX Reauthentication Request/Answer Command

This specification extends the Reauthentication-Request/Answer Command as defined in RFC3588 [54] due to the mandatory inclusions of the WiMAX-Session-Id AVP. As well, the Chargeable-User-Identity AVP is added to the commands; Chargeable-User-Identity as described in RFC 4372 [74], was completed after RFC3588 [54] was published.

#### WiMAX Reauthentication Request Command

The WiMAX Reauthentication Request Command (WRAR) is sent from the AAA in the CSN to the ASN to request that ASN reauthenticate or reauthorize the WiMAX session.

The command definition of the WRAR command is as follows:

<WRA-Request> ::= < Diameter Header: TBDWRA, REQ, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ Destination-Host }

{ Auth-Application-Id }

{ Re-Auth-Request-Type }

{ WiMAX-Session-Id }

[ User-Name ]

[ Chargeable-User-Identity ]

[ Origin-AAA-Protocol ]

[ Origin-State-Id ]

[ NAS-Identifier ]

[ NAS-IP-Address ]

[ NAS-IPv6-Address ]

[ NAS-Port ]

[ NAS-Port-Id ]

[ NAS-Port-Type ]

[ Service-Type ]

[ Framed-IP-Address ]

[ Framed-IPv6-Prefix ]

[ Framed-Interface-Id ]

[ Called-Station-Id ]

[ Calling-Station-Id ]

[ Originating-Line-Info ]

[ Acct-Session-Id ]

[ Acct-Multi-Session-Id ]

[ State ]

\* [ Class ]

[ Reply-Message ]

\* [ Proxy-Info ]

\* [ Route-Record ]

\* [ AVP ]

1

2

**Table 5-26 – Attributes of the WRAR command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
Re-Auth-Request-Type	285	Enumerated	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Origin-AAA-Protocol	408	Enumerated	RFC4005	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
NAS-Identifier	32	UTF8String	RFC4005	M	V
NAS-IP-Address	4	OctetString	RFC4005	M	V
NAS-IPv6-Address	95	OctetString	RFC4005	M	V
NAS-Port	5	Unsigned32	RFC4005	M	V
NAS-Port-Id	87	UTF8String	RFC4005	M	V
NAS-Port-Type	61	Enumerated	RFC4005	M	V
Service-Type	6	Enumerated	RFC4005	M	V
Framed-IP-Address	8	OctetString	RFC4005	M	V
Framed-IPv6-Prefix	97	OctetString	RFC4005	M	V
Framed-Interface-Id	96	Unsigned64	RFC4005	M	V
Called-Station-Id	30	UTF8String	RFC4005	M	V
Calling-Station-Id	31	UTF8String	RFC4005	M	V
Originating-Line-Info	94	OctetString	RFC4005		V
Accounting-Session-Id	44	OctetString	RFC3588	M	V
Acct-Multi-Session-Id	50	UTF8String	RFC3588	M	V
State	24	OctetString	RFC4005	M	V
Class	25	OctetString	RFC3588	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Reply-Message	18	UTF8String	RFC4005	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
WiMAX-Session-Id	4	OctetString	-	M,V	-
Chargeable-User-Identity	89	OctetString	RFC4372		V

The AAA server MUST include the Chargeable-User-Identity AVP in a RAR command, if there was indication that the Chargeable-User-Identity attribute is to be used for the session (see DER/DEA command); in this case the M-bit of the Chargeable-User-Identity AVP MUST be set. Otherwise, the Chargeable-User-Identity AVP SHOULD NOT be sent, but if sent, the Chargeable-User-Identity's M-bit MUST be cleared.

### WiMAX Reauthentication Answer (WRAA) Command

The WiMAX Reauthentication Request Command (WRAA) is sent from the NAS to the AAA in response of receipt of the WRAR command.

The command definition of the WRAA command is as follows:

<WRA-Answer> ::= < Diameter Header: TBDWRA, PXY >

< Session-Id >

{ Result-Code }

{ Origin-Host }

{ Origin-Realm }

[ User-Name ]

[ Origin-AAA-Protocol ]

[ Origin-State-Id ]

[ Error-Message ]

[ Error-Reporting-Host ]

\* [ Failed-AVP ]



\* [ Redirected-Host ]

[ Redirected-Host-Usage ]

[ Redirected-Host-Cache-Time ]

[ Service-Type ]

\* [ Configuration-Token ]

[ Idle-Timeout ]

[ Authorization-Lifetime ]

[ Auth-Grace-Period ]

[ Re-Auth-Request-Type ]

[ State ]

\* [ Class ]

\* [ Reply-Message ]

[ Prompt ]

\* [ Proxy-Info ]

\* [ AVP ]

1

2

**Table 5-27 – Attributes of the WRAA command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V

123  
4  
5  
6

## 7

8  
9  
10  
11

## 12

13  
14  
15

16

17

{ Termination-Cause }  
 { WiMAX-Session-Id }  
 [ User-Name ]  
 [ Chargeable-User-Identity ]  
 [ Destination-Host ]  
 \* [ Class ]  
 [ Origin-AAA-Protocol ]  
 [ Origin-State-Id ]  
 \* [ Proxy-Info ]  
 \* [ Route-Record ]  
 \* [ AVP ]

**Table 5-28 – Attributes of the WSTR command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Origin-AAA-Protocol	408	Enumerated	RFC4005	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Class	25	OctetString	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
WiMAX-Session-Id	4	OctetString	-	M,V	
Chargeable-User-Identity	89	OctetString	RFC4372		V

## WiMAX Session Termination Answer (WSTA) command

The WiMAX Session Termination Answer command (WSTA) is sent from the AAA to the ASN to acknowledge receipt of a WSTR command. WiMAX Session Termination Answer (WSTA) command definition follows:

```
<WST-Answer> ::= < Diameter Header: TBDWST, PXY >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { WiMAX-Session-Id }
    [ User-Name ]
    [ Chargeable-User-Identity ]
    * [ Class ]
    [ Error-Message ]
    [ Error-Reporting-Host ]
    * [ Failed-AVP ]
    [ Origin-AAA-Protocol ]
    [ Origin-State-Id ]
    * [ Redirect-Host ]
    [ Redirect-Host-Usage ]
    [ Redirect-Max-Cache-Time ]
    * [ Proxy-Info ]
    * [ AVP ]
```

**Table 5-29 – Attributes of the WSTA command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Result-Code	268	Unsigned32	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Chargeable-User-Identity	89	OctetString	RFC4372	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V
Framed-IP-Address	8	OctetString	RFC4005	M	V
NAS-Filter-Rule	400	IPFilterRule	RFC4005	M	V
Error-Message	281	UTF8String	RFC3588		V,M
Error-Reporting-Host	294	DiamIdentity	RFC3588		V,M
Failed-AVP	279	Grouped	RFC3588	M	V
Redirect-Host	292	DiamURI	RFC3588	M	V
Redirect-Host-Usage	261	Enumerated	RFC3588	M	V
Redirect-Host-Cache-Time	262	Unsigned32	RFC3588	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
WiMAX-Session-Id	4	OctetString	-	M,V	
Chargeable-User-Identity	89	OctetString	RFC4372		V

#### 5.5.1.1.5 WiMAX Abort Session Request/Answer Command

This specification extends the Abort Session Request/Answer commands as defined in RFC3588 [54] due to the mandatory inclusions of the WiMAX-Session-Id AVP. As well, the Chargeable-User-Identity AVP is added to the commands; Chargeable-User-Identity as described in RFC 4372 [74], was completed after RFC3588 [54] was published.

#### WiMAX Abort Session Request (WASR) command

The WASR is sent from the AAA server to the ASN to request that the specified session terminate. WiMAX Abort Session Termination Request (WASR) command definition follows:

```
<WAS-Request> ::= < Diameter Header: TBDWAS, REQ, PXY >
    < Session-Id >
    { Origin-Host }
    { Origin-Realm }
```

{ Destination-Realm }  
 { Destination-Host }  
 {Auth-Application-Id}  
 { WiMAX-Session-Id }  
 [ User-Name ]  
 [ Chargeable-User-Identity ]  
 [ Origin-AAA-Protocol ]  
 [ Origin-State-Id ]  
 [ NAS-Identifier ]  
 [ NAS-IP-Address ]  
 [ NAS-IPv6-Address ]  
 [ NAS-Port ]  
 [ NAS-Port-Id ]  
 [ NAS-Port-Type ]  
 [ Service-Type ]  
 [ Framed-IP-Address ]  
 [ Framed-IPv6-Prefix ]  
 [ Framed-Interface-Id ]  
 [ Called-Station-Id ]  
 [ Calling-Station-Id ]  
 [ Originating-Line-Info ]  
 [ Accounting-Session-Id ]  
 [ Acct-Multi-Session-Id ]  
 [ State ]  
 \* [ Class ]  
 \* [ Reply-Message ]  
 \* [ Proxy-Info ]  
 \* [ Route-Record ]  
 \* [ AVP ]

1

2

**Table 5-30 – Attributes of the WASR command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
Re-Auth-Request-Type	285	Enumerated	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Origin-AAA-Protocol	408	Enumerated	RFC4005	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
NAS-Identifier	32	UTF8String	RFC4005	M	V
NAS-IP-Address	4	OctetString	RFC4005	M	V
NAS-IPv6-Address	95	OctetString	RFC4005	M	V
NAS-Port	5	Unsigned32	RFC4005	M	V
NAS-Port-Id	87	UTF8String	RFC4005	M	V
NAS-Port-Type	61	Enumerated	RFC4005	M	V
Service-Type	6	Enumerated	RFC4005	M	V
Framed-IP-Address	8	OctetString	RFC4005	M	V
Framed-IPv6-Prefix	97	OctetString	RFC4005	M	V
Framed-Interface-Id	96	Unsigned64	RFC4005	M	V
Called-Station-Id	30	UTF8String	RFC4005	M	V
Calling-Station-Id	31	UTF8String	RFC4005	M	V
Originating-Line-Info	94	OctetString	RFC4005		V
Accounting-Session-Id	44	OctetString	RFC3588	M	V
Acct-Multi-Session-Id	50	UTF8String	RFC3588	M	V
State	24	OctetString	RFC4005	M	V
Class	25	OctetString	RFC3588	M	V
Reply-Message	18	UTF8String	RFC4005	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V
Service-Type	6	Enumerated	RFC4005	M	V

1  
2

AVP Name	AVP	Value	Reference	AVP Flag rules
----------	-----	-------	-----------	----------------

	Code	Type		Must	Must not
WiMAX-Session-Id	4	OctetString		M,V	
Chargeable-User-Identity	89	OctetString	RFC4372		V

## WiMAX Abort Session Answer (WASA) command

The WASA is sent from the NAS to the AAA server to acknowledge the receipt of a WASR command. WiMAX Abort Session Termination Request (WASA) command definition follows:

<WAS-Answer> ::= < Diameter Header: TBDWAS, PXY >

< Session-Id >

{ Result-Code }

{ Origin-Host }

{ Origin-Realm }

{ WiMAX-Session-Id }

[ User-Name ]

[ Chargeable-User-Identity ]

[ Origin-AAA-Protocol ]

[ Origin-State-Id ]

[ State]

[ Error-Message ]

[ Error-Reporting-Host ]

\* [ Failed-AVP ]

\* [ Redirected-Host ]

[ Redirected-Host-Usage ]

[ Redirected-Max-Cache-Time ]

\* [ Proxy-Info ]

\* [ AVP ]

**Table 5-31 – Attributes of the WASA command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Result-Code	268	Unsigned32	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V



AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Chargeable-User-Identity	89	OctetString	RFC4372	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V
Framed-IP-Address	8	OctetString	RFC4005	M	V
NAS-Filter-Rule	400	IPFilterRule	RFC4005	M	V
Error-Message	281	UTF8String	RFC3588		V,M
Error-Reporting-Host	294	DiamIdentity	RFC3588		V,M
Failed-AVP	279	Grouped	RFC3588	M	V
Redirect-Host	292	DiamURI	RFC3588	M	V
Redirect-Host-Usage	261	Enumerated	RFC3588	M	V
Redirect-Host-Cache-Time	262	Unsigned32	RFC3588	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
WiMAX-Session-Id	4	OctetString		M,V	
Chargeable-User-Identity	89	OctetString	RFC4372		V

#### 5.5.1.2 WiMAX MIP4 Diameter Application

The WiMAX MIP4 Diameter Application is derived from the Diameter MIP Application RFC4004 [61].

The WiMAX MIP4 Diameter Application exchanges messages between the HA and the AAA server. The following table lists all of the commands that MUST be supported by a node claiming to support the WiMAX MIP4 Diameter Application:

Command-Name	Abbrev.	Code
WiMAX-Home-Agent-IPv4-Request	WHA4R	<IANA Pending> WHA4
WiMAX-Home-Agent-IPv4-Answer	WHA4A	<IANA Pending> WHA4

Command-Name	Abbrev.	Code
WiMAX-Change-of-Authorization-Request	WCAR	<IANA Pending> WCA
WiMAX-Change-of-Authorization-Answer	WCAA	<IANA Pending> WCA
WiMAX-Session-Termination-Request	WSTR	<IANA Pending> WST
WiMAX-Session-Termination-Answer	WSTA	<IANA Pending> WST
WiMAX-Abort-Session-Request	WASR	<IANA Pending> WAS
WiMAX-Abort-Session-Answer	WASA	<IANA Pending> WAS

The following commands are reused from the WiMAX Network Access Authentication and Authorization Diameter Application (see <IANA Pending>). The Auth-Application-Id AVP in these commands MUST be set to <IANA Pending> WM4DA.

- WiMAX-Change-of-Authorization-Request, (WCAR)
- WiMAX-Change-of-Authorization-Answer, (WCAA)
- WiMAX-Session-Termination-Request, (WSTR)
- WiMAX-Session-Termination-Answer, (WSTA)
- WiMAX-Abort-Session-Request, (WASR)
- WiMAX-Abort-Session-Answer, (WASA)

#### 5.5.1.2.1 WiMAX-Home-Agent-IPv4-Request /Answer Command

The WiMAX-Home-Agent-IPv4-Request /Answer commands are interchanged between the HA and the HAAA and in the case of allocation of HA in a visited CSN will involve the VAAA.

The commands are exchanged in order to provide the HA with keys necessary to validate the Mobility Authentication extensions.

#### WiMAX-Home-Agent-IPv4-Request (WHA4R) Command

The WiMAX-Home-Agent-IPv4-Request command is sent from the HA providing Mobile IPv4 service to the HAAA upon the HA receiving a MIP4 Registration Request message.

<WHA4R> ::= <Diameter Header: TBDWHA4, REQ, PXY>

<Session-Id>

{ Auth-Application-Id }

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ Auth-Request-Type }

Auth-Request-Type value MUST be set to AUTHORIZE\_ONLY (2) as defined in RFC3588 [54]

{ WiMAX-Capability }

{ User-Name }

{ MIP-MN-HA-SPI }	Contains the SPI of the MN-HA being requested.
{ hHA-IPv4 }	HA-IP of the HA as seen from the MS.
{ RRQ-HA-IP }	IPv4 address of the HA as found in the MIP Registration Request
[ HA-RK-SPI ]	MUST be included and set to the SPI contained in the FA-HA Authentication Extension, if received in the MIP Registration Request
[ Destination-Host ]	
[ Origin-State-Id ]	
[ Auth-Session-State ]	
[ WiMAX-Session-Id ]	Once the HA receives a WiMAX-Session-Id the HA MUST included the WiMAX-Session-Id in all subsequent WMHR message for this session
[ Framed-IP-Address ]	Set to the Home Address received in the MIP-Registration Request
[ MIP-Feature-Vector ]	
[ Chargeable-User-Identity ]	MAY be included by the HA in the initial request message for this session. MUST be included in subsequent commands if received a Chargeable-User-Identity for this session.
*[Proxy-Info]	
*[Route-Record]	
*[AVP]	

**Table 5-32 – Attributes of the WHA4R command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Chargeable-User-Identity	89	OctetString	RFC4372	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V
WiMAX-Capability	1	Grouped		M,V	
WiMAX-Session-Id	4	OctetString		M,V	
MN-HA-MIP4-SPI	11	Unsigned32	SPLIT	M	V
hHA-IPv4	6	Address		M,V	
RRQ-HA-IP	18	Address		M,V	
HA-RK-SPI	16	Unsigned32		M,V	
Framed-IP-Address	8	OctetString	RFC4005	M	V
MIP-Feature-Vector	337	Unsigned32	RFC3588	M	V
Auth-Request-Type	274	Enumerated	RFC3588	M	V
Auth-Session-State	277	Enumerated	RFC3588	M	V

1

## 2 **WiMAX-Home-Agent-IPv4-Answer (WHA4A) Command**

3 This command is sent by the AAA to the HA in response to a WMHAR command. The following specifies the  
4 allowed AVP in the command:

5 <WHA4A> ::= < Diameter Header: TBD WHA4, PXY >

<Session-Id>

{ Auth-Application-Id }

{ Result-Code }

{ Origin-Host }

{ Origin-Realm }

{ WiMAX-Capability }

{ WiMAX-Session-Id }

[ MN-HA-MIP4-MSA ]

Contains the MN-HA key that corresponds to the MN-HA SPI that was requested in the WHA4R command.

MUST be returned unless there is a failure.

[ User-Name ]

[ Origin-State-Id ]

[ MIP-Feature-Vector ]

[ Framed-IP-Address ]

The Home Address assigned to the mobile.

[ RRQ-MN-HA-KEY ]

Only needed if the HA-IP of the HA is

	different than the HA-IP address in MIP Registration Request as received in the MIP-RRQ-HA-IPv4
[ HA-RK-MSA ]	MUST be included by the AAA that is assigning the HA-RK-MSA for the HA, if a HA-RK-SPI was received in the associated WHA4R.
[ Class ]	
[ Chargeable-User-Identity ]	The Chargeable-User-Identity AVP MUST be included if the Chargeable-User-Identity was included in the corresponding WMHAR command.
[ Acct-Interim-Interval ]	
* [ NAS-Filter-Rule ]	
[ Hotline-Profile-ID ]	
* [ HTTP-Redirection-Rule ]	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.
* [ IP-Redirection-Rule ]	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.
* [ Hotline-Session-Timer ]	
[ Hotline-Indication ]	If the session is to be Hot-Lined then this attribute SHALL be specified and the HA SHALL include this attribute in the accounting messages.
[ Error-Message ]	
[ Error-Reporting-Host ]	
* [ Failed-AVP ]	
[ Re-Auth-Request-Type ]	
* [ Redirected-Host ]	
[ Redirected-Host-Usage ]	
[ Redirected-Max-Cache-Time ]	
*[Proxy-Info ]	
*[Route-Record ]	
*[ AVP ]	

1

**Table 5-33 – Attributes of the WHA4A command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Result-Code	268	Unsigned32	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Chargeable-User-Identity	89	OctetString	RFC4372	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V
Framed-IP-Address	8	OctetString	RFC4005	M	V
NAS-Filter-Rule	400	IPFilterRule	RFC4005	M	V
Error-Message	281	UTF8String	RFC3588		V,M
Error-Reporting-Host	294	DiamIdentity	RFC3588		V,M
Failed-AVP	279	Grouped	RFC3588	M	V
Redirect-Host	292	DiamURI	RFC3588	M	V
Redirect-Host-Usage	261	Enumerated	RFC3588	M	V
Redirect-Max-Cache-Time	262	Unsigned32	RFC3588	M	V
WiMAX-Capability	1	Grouped		M,V	
WiMAX-Session-Id	4	OctetString		M,V	
Acct-Interim-Interval	85	Unsigned32	RFC3588	M	V
MN-HA-MIP4-MSA	328	Grouped		M,V	
HA-RK-MSA	331	Grouped		M,V	
Hotline-Profile-ID	53	UTF8String		M,V	
HTTP-Redirection-Rule	54	Grouped		M,V	
IP-Redirection-Rule	55	Grouped		M,V	
NAS-Filter-Rule	92		4005	M	V
Hotline-Session-Timer	56	Unsigned32		M,V	
Hotline-Indication	24	UTF8String		M,V	
MIP-Feature-Vector	337	Unsigned32	RFC3588	M	V
RRQ-MN-HA-KEY	19	OctetString		M,V	

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Class	25	OctetString		M	V
Re-Auth-Request-Type	285	Enumerated		M	V

### 5.5.1.3 WiMAX MIP6 Diameter Application

The WiMAX MIP6 Diameter Application is based on the application defined in draft-ietf-dime-mip6-split-10.txt [84].

The following table lists all of the commands that are applicable to the WiMAX Network Access Authentication and Authorization Diameter Application:

Command-Name	Abbrev.	Code
WiMAX-Home-Agent-IPv6-Request	WHA6R	<IANA Pending>WHA6
WiMAX-Home-Agent-IPv6-Answer	WHA6A	<IANA Pending>WHA6
WiMAX-Change-of-Authorization-Request	WCAR	<IANA Pending>WCA
WiMAX-Change-of-Authorization-Answer	WCAA	<IANA Pending>WCA
WiMAX-Session-Termination-Request	WSTR	<IANA Pending>WST
WiMAX-Session-Termination-Answer	WSTA	<IANA Pending>WST
WiMAX-Abort-Session-Request	WASR	<IANA Pending>WAS
WiMAX-Abort-Session-Answer	WASA	<IANA Pending>WAS

The following commands are reused from the WiMAX Network Access Authentication and Authorization Diameter Application (see Table 5-16). The Auth-Application-Id AVP in these commands MUST be set to <IANA Pending>WM6DA.

- WiMAX-Change-of-Authorization-Request, (WCAR)
- WiMAX-Change-of-Authorization-Answer, (WCAA)
- WiMAX-Session-Termination-Request, (WSTR)
- WiMAX-Session-Termination-Answer, (WSTA)
- WiMAX-Abort-Session-Request, (WASR)
- WiMAX-Abort-Session-Answer, (WASA)

### 5.5.1.3.1 WiMAX MIP6 Request/Answer Commands

The WiMAX MIP6 Request/Answer commands are interchanged between the HA and the HAAA and in the case of allocation of HA in a visited CSN will involve the VAAA.

The commands are exchanged in order to provide the HA with keys necessary to validate the MIP6 Binding Update message.

#### WiMAX MIP6 Request Command (WMIP6R)

The WiMAX MIP6 Request command is sent from the HA providing Mobile IPv6 service to the HAAA (optionally via VAAA in the case that HA is in the VCSN) upon the HA receiving a MIP6 Binding Update message.

< WiMAX-Home-Agent-IPv6-Request > ::= < Diameter Header: TBD WHA6,REQ, PXY>

< Session-Id >

{Auth-Application-Id}

{ User-Name }

{ Destination-Realm }

{ Origin-Host }

{ Origin-Realm }

{ Auth-Request-Type }

Auth-Request-Type value MUST be set to AUTHORIZE\_ONLY (2) as defined in RFC3588 [54]

{ MIP-MN-HA-SPI }

{ MIP-Mobile-Node-Address }

{ MIP-Home-Agent-Address }

{ MIP-Careof-Address }

{ WiMAX-Capability }

[ Destination-Host ]

[ Origin-State-Id ]

[ WiMAX-Session-Id ]

Once the HA receives a WiMAX-Session-Id the HA MUST included the WiMAX-Session-Id in all subsequent WMHR message for this session.

[ Service-Selection ]

[ MIP6-Feature-Vector ]

[ Chargeable-User-Identity ]

MAY be included by the HA in the initial request message for this session. MUST be included in subsequent commands if received a Chargeable-User-Identity for this session.

[ Auth-Session-State ]

\* [ Proxy-Info ]

\* [ Route-Record ]



\* [ AVP ]

**Table 5-34 – Attributes of the WHA6R command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Destination-Realm	283	DiamIdentity	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Chargeable-User-Identity	89	OctetString	RFC4372	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V
Service-Selection	TBD	TBD	SPLIT	M	V
WiMAX-Capability	1	Grouped		M,V	
WiMAX-Session-Id	4	OctetString		M,V	
MIP-Home-Agent-Address	334	Address	RFC3588	M,V	
MIP6-Feature-Vector	TBD	Unsigned64	SPLIT	M	V
Auth-Request-Type	274	Enumerated	RFC3588	M	V
Auth-Session-State	277	Enumerated	RFC3588	M	V
MIP-MN-HA-SPI	TBD		SPLIT	M	V
MIP-Mobile-Node-Address	333	Address	RFC3588	M	V
MIP-Careof-Address	TBD	Address	SPLIT	M	V

#### WiMAX MIP6 Answer Command (WMIP6A)

The WiMAX MIP6 Answer command is sent from the HAAA to the HA in response to the receipt of a WiMAX MIP6 Request Command.

< WiMAX-Home-Agent-IPv6-Answer > ::= < Diameter Header: TBD WHA6 PXY >

< Session-Id >

{ Result-Code }

{ Origin-Host }	
{ Origin-Realm }	
{ WiMAX-Capability }	
{ WiMAX-Session-Id }	
[ User-Name ]	
[ Authorization-Lifetime ]	
[ Auth-Session-State ]	
[ Error-Message ]	
[ Error-Reporting-Host ]	
* [Failed-AVP ]	
[ Re-Auth-Request-Type ]	
[ Acct-Interim-Interval ]	
[ MIP6-Feature-Vector ]	
[ MIP-Mobile-Node-Address ]	
[ MN-HA-MSA ]	MUST be returned unless there is a failure.
[ Chargeable-User-Identity ]	The Chargeable-User-Identity AVP MUST be included if the Chargeable-User-Identity was included in the corresponding WMIP6R command.
[ Class ]	
[ Hotline-Profile-ID ]	
* [ HTTP-Redirection-Rule ]	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.
* [ IP-Redirection-Rule ]	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.
* [ Hotline-Session-Timer ]	
[ Hotline-Indication ]	If the session is to be Hot-Lined then this attribute SHALL be specified and the HA SHALL include this attribute in the accounting messages.
* [ Redirected-Host ]	
[ Redirected-Host-Usage ]	
[ Redirected-Max-Cache-Time ]	

[ Origin-State-Id ]

\* [ Proxy-Info ]

\*[Route-Record ]

\* [ AVP ]

1

2

**Table 5-35 – Attributes of the WHA6A command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Result-Code	268	Unsigned32	RFC3588	M	V
Origin-Host	264	DiamIdent	RFC3588	M	V
Origin-Realm	296	DiamIdent	RFC3588	M	V
User-Name	1	UTF8String	RFC3588	M	V
Authorization-Lifetime	291	Unsigned32	RFC3588	M	V
Auth-Session-State	277	Enumerated	RFC3588	M	V
Error-Message	281	UTF8String	RFC3588		M,V
Error-Reporting-Host	294	DiamIdent	RFC3588		M,V
Failed-AVP	279	Grouped	RFC3588	M	V
Re-Auth-Request-Type	285	Enumerated	RFC3588	M	V
Acct-Interim-Interval	85	Unsigned32	RFC3588	M	V
Chargeable-User-Identity	89	OctetString	RFC3588	M	V
Class	25	OctetString	RFC3588	M	V
Redirected-Host	292	DiamURI	RFC3588	M	V
Redirected-Host-Usage	261	Enumerated	RFC3588	M	V
Redirected-Max-Cache-Time	262	Unsigned32	RFC3588	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdent		M	V
MIP6-Feature-Vector	TBD	Unsigned64	TBDSPLIT	M	V
MIP-Mobile-Node-Address	333	Address	RFC3588	M	V
WiMAX-Capability	1	Grouped		M,V	
WiMAX-Session-Id	4	OctetString		M,V	
MIP-MN-HA-MSA	TBD	Grouped	TBDSPLIT	M	V

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Hotline-Profile-ID	53	UTF8String		M,V	
HTTP-Redirection-Rule	54	Grouped		M,V	
IP-Redirection-Rule	55	Grouped		M,V	
Hotline-Session-Timer	56	Unsigned32		M,V	
Hotline-Indication	24	UTF8String		M,V	

#### 5.5.1.4 WiMAX DHCP Diameter Application

The WiMAX DHCP Diameter Application is derived from the Diameter Base Application RFC3588 [54].

Messages exchanged as part of the WiMAX DHCP Diameter Application MUST have their Auth-Application-Id AVP set to TBDWDDA.

The WiMAX DHCP Diameter Application exchanges message between the DHCP server and the AAA server. The following table lists all of the commands that MUST be supported by a node claiming to support the WiMAX DHCP Diameter Application:

Command-Name	Abbrev.	Code
WiMAX-DHCP-Request	WDHCPR	TBDWDHCP
WiMAX-DHCP-Answer.	WDHCPA	TBDWDHCP

The WiMAX DHCP Diameter Application is stateless and thus does not require Session Termination Request/Answers. As well, when the DHCP Root Key lifetime expires the DHCP Server will not require to re-authorize the key. Instead, it is expected that the DHCP Server will receive a new Key Identifier corresponding to a fresh key.

##### 5.5.1.4.1 WiMAX DHCP Request/Answer Commands

The WiMAX DHCP Request/Answer commands are used by the DHCP Server to fetch a DHCP Root Key identified by the DHCP-RK-Key-ID AVP.

#### WiMAX DHCP Request command

The WiMAX DHCP Request command is used by the DHCP Server to fetch the key identified by the DHCP-RK-Key-ID AVP. The DHCP Server MUST include its IP address as seen by the DHCP Clients.

< WDHCPR > ::= <Diameter Header: TBDWDHCP, REQ,PXY>

<Session-Id>

{ Auth-Application-Id }

{ Origin-Host }

{ Origin-Realm }

{ Auth-Request-Type }      Auth-Request-Type value MUST be set to AUTHORIZE\_ONLY (2) as defined in RFC3588 [54]

{ DHCP-RK-Key-ID }      The key ID as received in the DHCPDISCOVER message

{ DHCPMSG-Server-IP }      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 than the address contained in the DHCP-Server-IPv4 attribute.

[ Destination-Host ]

[ Origin-State-Id ]

[ Auth-Session-State ]

If included MUST be set to “NO\_STATE\_MAINTAINED”  
(1)

\*[Proxy-Info]

\*[Route-Record]

\*[AVP]

**Table 5-36 – Attributes of the WDHCP command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Auth-Application-Id	258	Unsigned32	RFC3588	M	V
Origin-Host	264	DiamIdentity	RFC3588	M	V
Origin-Realm	296	DiamIdentity	RFC3588	M	V
Auth-Request-Type	274	Enumerated	RFC3588	M	V
Auth-Session-State	277	Enumerated	RFC3588	M	V
Destination-Host	293	DiamIdentity	RFC3588	M	V
Origin-State-Id	278	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdentity	RFC3588	M	V
DHCP-RK-Key-ID	41	Unsigned32		M,V	
DHCPMSG-Server-IP	43	Address		M,V	

### WiMAX DHCP Answer command

The WiMAX DHCP Answer command is sent from the HAAA to the DHCP server to deliver the DHCP root key that corresponds to the DHCP-RK-Key-ID received in the WDHCP command.

< WDHCP > ::= < Diameter Header: TBD WDHCP, PXY >

<Session-Id>

{ Result-Code }

{ Origin-Host }

{ Origin-Realm }

{ Auth-Session-State } MUST be set to “NO\_STATE\_MAINTAINED”

[ DHCP-RK-SA ] Upon success result the DHCP RK Security association containing the Key ID as received in the WDHCP command, the associated root key and its lifetime MUST be included in this command

[ Error-Message ]

[ Error-Reporting-Host ]

\* [ Failed-AVP ]

\* [ Redirected-Host ]

[ Redirected-Host-Usage ]

[ Redirected-Max-Cache-Time ]

\*[Proxy-Info ]

\*[Route-Record ]

\*[ AVP ]

**Table 5-37 – Attributes of the WDHCPA command**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC3588	M	V
Result-Code	268	Unsigned32	RFC3588	M	V
Origin-Host	264	DiamIdent	RFC3588	M	V
Origin-Realm	296	DiamIdent	RFC3588	M	V
Auth-Session-State	277	Enumerated	RFC3588	M	V
Error-Message	281	UTF8String	RFC3588		M,V
Error-Reporting-Host	294	DiamIdent	RFC3588		M,V
Failed-AVP	279	Grouped	RFC3588	M	V
Redirected-Host	292	DiamURI	RFC3588	M	V
Redirected-Host-Usage	261	Enumerated	RFC3588	M	V
Redirected-Max-Cache-Time	262	Unsigned32	RFC3588	M	V
Proxy-Info	284	Grouped	RFC3588	M	V
Route-Record	282	DiamIdent	RFC3588	M	V
DCHP-RK-SA	333	Grouped		M,V	

### 5.5.1.5 Messages for Online-Accounting

Online charging messages are based directly on the format of the messages defined in IETF RFC 4006 [63] and modified in TS32.299 [99]. In the definition of the Diameter Commands, the AVPs that are specified in the referenced specifications but not used by the WiMAX charging specifications are marked with strikethrough.

#### 5.5.1.5.1 Initialization, maintenance and termination of connection and session

The initialization and maintenance of the connection between the PPC and PPS pairs are described in RFC3588 [54].

After establishing the transport connection, the PPC and the PPS SHALL advertise the support of the R3-OC specific application by including the value of the WiMAX application identifier in the Auth-Application-Id AVP [WiMAX-PCC] and the value of WiMAX (24757) in the Vendor-Id AVP of the Vendor-Specific-Application-Id AVP contained in the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. The PPC and PPS SHALL advertise support of WiMAX and 3GPP vendor-specific AVPs by including the vendor identifier value of WiMAX (24757) within a Supported-Vendor-Id AVP, and the vendor identifier value of 3GPP (10415) within a Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in the Diameter Base Protocol (RFC 3588 [54]).

The termination of the Diameter user session is specified in RFC 3588 [54]. The description of how to use these termination procedures in the normal cases is embedded in the procedures description.

#### 5.5.1.5.2 R3-OC Auth-Application-ID

A new vendor specific Diameter Auth-Application-ID is defined for WiMAX.

The R3-OC application is defined as vendor specific Diameter application, where the vendor is WiMAX. The Diameter Auth-Application-ID is assigned by <http://www.iana.org/assignments/aaa-parameters> registry (per RFC3588 [54]) under Applications IDs.

#### 5.5.1.5.3 Credit-Control-Request message

The Credit-Control-Request message (CCR) is indicated by the command-code field being set to 272 and the 'R' bit being set in the Command Flags field. It is used between the Diameter credit-control client and the credit-control server to request credits for the request bearer/subsystem/service.

Message format:

<CCR> ::= < Diameter Header: 272, REQ, PXY >

{ Origin-Host }  
{ Origin-Realm }  
{ Destination-Realm }  
{ Auth-Application-Id }  
{ Service-Context-Id }  
{ CC-Request-Type }  
{ CC-Request-Number }  
[ Destination-Host ]  
[ User-Name ]  
[ CC-Sub-Session-Id ]  
[ Acct-Multi-Session-Id ]

- [ Origin-State-Id ]
- [ Event-Timestamp ]
- \* [ Subscription-Id ]
- [ Service-Identifier ]
- [ Termination-Cause ]
- [ Requested-Service-Unit ]
- [ Requested-Action ]
- [ Used-Service-Unit ]
- [ Multiple-Services-Indicator ]
- \* [ Multiple-Services-Credit-Control ]
- [ Service-Parameter-Info ]
- [ CC-Correlation-Id ]
- [ User-Equipment-Info ]
- \* [ Proxy-Info ]
- \* [ Route-Record ]
- [ Service-Information ]
- \* [ AVP ]

1  
2 Table 5-38 illustrates the basic structure of Diameter Credit Control Credit-Control-Request message as used for  
3 Online Charging.

4 **Table 5-38 – Credit-Control-Request Message Content**

AVP	Category	Description
Session-Id	M	This field identifies the operation session.
Origin-Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Origin-Realm	M	This field contains the realm of the operation originator.
Destination-Realm	M	This field contains the realm of the operator domain. The realm will be addressed with the domain address of the corresponding public URI.
Auth-Application-Id	M	This field corresponds to the application ID of the Diameter Credit Control Application and is defined with the value 4.
Service-Context-Id	M	This field contains a unique identifier of the Diameter credit-control service specific document that applies to the request.
CC-Request-Type	M	This field defines the transfer type: event for event based charging and initial, update, terminate for session based charging.



CC-Request-Number	M	This field contains the sequence number of the transferred messages.
Destination-Host	O <sub>C</sub>	This field contains the destination peer address of the OCS identity.
User-Name	O <sub>C</sub>	This field contains the User-Name, in a format consistent with the NAI specification.
CC-Sub-Session-Id	-	Not used in WiMAX.
Acct-Multi-Session-Id	O <sub>C</sub>	
Origin-State-Id	O <sub>C</sub>	This field contains the state associated to the Charging Trigger Function (CTF).
Event-Timestamp	O <sub>C</sub>	This field corresponds to the exact time the quota is requested.
Subscription-Id	O <sub>M</sub>	This field contains the identification of the user that is going to access the service in order to be identified by the OCS.
Subscription-Id-Type	M	This field determines the type of the identifier, e.g. END_USER_NAI for WiMAX
Subscription-Id-Data	M	This field contains the user data content, e.g. NAI for WiMAX.
Service-Identifier	O <sub>C</sub>	Not used in WiMAX.
Termination-Cause	O <sub>C</sub>	This field contains the reason the credit control session was terminated.
Requested-Service-Unit	-	Not used in WiMAX, see Multiple-Services-Credit-Control.
CC-Time	-	
CC-Money	-	
Unit-Value	-	
Value-Digits	-	
Exponent	-	
Currency-Code	-	
CC-Total-Octets	-	
CC-Input-Octets	-	
CC-Output-Octets	-	
CC-Service-Specific-Units	-	
AVP	-	
Requested-Action	O <sub>C</sub>	The field defines the type of action if the CC-Request-Type indicates EVENT.
Used-Service-Unit	-	Not used in WiMAX, see Multiple-Services-Credit-Control.
Tariff-Change-Usage	-	

CC-Time	-	
CC-Money	-	
Unit-Value	-	
Value-Digits	-	
Exponent	-	
Currency-Code	-	
CC-Total-Octets	-	
CC-Input-Octets	-	
CC-Output-Octets	-	
CC-Service-Specific-Units	-	
AVP	-	
Multiple-Services-Indicator	O <sub>M</sub>	This field indicates whether the CTF is capable of handling multiple services independently.
Multiple-Services-Credit Control	O <sub>C</sub>	This field contains all parameters for the CTF quota management and defines the quotas to allow traffic to flow.
Granted-Service-Unit	-	Not used in CCR.
Tariff-Change-Usage	-	
CC-Time	-	
CC-Money	-	
Unit-Value	-	
Value-Digits	-	
Exponent	-	
Currency-Code	-	
CC-Total-Octets	-	
CC-Input-Octets	-	
CC-Output-Octets	-	
CC-Service-Specific-Units	-	
AVP	-	
Requested-Service-Unit	O <sub>C</sub>	This field contains the amount of requested service units for a particular category or an indication that units are needed for a particular category, as defined in [RFC4006].
CC-Time	O <sub>C</sub>	This field contains the amount of requested time.
CC-Money	-	Not used in WiMAX.
Unit-Value	-	
Value-Digits	-	
Exponent	-	

Currency-Code	-	
CC-Total-Octets	O <sub>C</sub>	This field contains the requested amount of octets to be sent and received.
CC-Input-Octets	O <sub>C</sub>	This field contains the requested amount of octets to be received.
CC-Output-Octets	O <sub>C</sub>	This field contains the requested amount of octets to be sent.
CC-Service-Specific-Units	O <sub>C</sub>	This field contains the requested amount of service specific units, e.g. number of events.
AVP	O <sub>C</sub>	
Used-Service-Unit	O <sub>C</sub>	This field contains the amount of used non-monetary service units measured for a particular category to a particular quota type.
Reporting-Reason	O <sub>C</sub>	
Tariff-Change-Usage	O <sub>C</sub>	This field identifies the reporting period for the used service unit, i.e. before, after or during tariff change.
CC-Time	O <sub>C</sub>	This field contains the amount of used time.
CC-Money	-	Not used in WiMAX.
Unit-Value	-	
Value-Digits	-	
Exponent	-	
Currency-Code	-	
CC-Total-Octets	O <sub>C</sub>	This field contains the amount of sent and received octets.
CC-Input-Octets	O <sub>C</sub>	This field contains the amount of received octets.
CC-Output-Octets	O <sub>C</sub>	This field contains the amount of sent octets.
CC-Service-Specific-Units	O <sub>C</sub>	This field contains the amount of service specific units, e.g. number of events.
AVP	O <sub>C</sub>	
Tariff-Change-Usage	-	Not used in CCR.
Service-Identifier	O <sub>C</sub>	This field contains identity of the used service. This ID with the Service-Context-ID together forms a unique identification of the service.
Rating-Group	O <sub>C</sub>	This field contains the identifier of a rating group.
G-S-U-Pool-Reference	-	Not used in CCR.
G-S-U-Pool-Identifier	-	
CC-Unit-Type	-	
Unit-Value	-	
Value-Digits	-	

Exponent	-	
Validity-Time	-	Not used in CCR.
Result-Code	-	Not used in CCR.
Final-Unit-Indication	-	Not used in CCR.
Final-Unit-Action	-	
Restriction-Filter-Rule	-	
Filter-Id	-	
Redirect-Server	-	
Redirect-Address-Type	-	
Redirect-Server-Address	-	
Time-Quota-Mechanism	O <sub>C</sub>	
Time-Quota-Type	M	
Trigger	O <sub>C</sub>	Used as defined in [99].
Trigger-Type	O <sub>C</sub>	Used as defined in [99].
AVP	O <sub>C</sub>	
Service-Parameter-Info	-	Not used in WiMAX.
Service-Parameter-Type	-	
Service-Parameter-Value	-	
CC-Correlation-Id	-	Not used in WiMAX.
User-Equipment-Info	O <sub>C</sub>	This field contains the identification of the identity and terminal capability the subscriber is using for the connection to mobile network if available.
User-Equipment-Info-Type	M	This field determines the type of the identifier.
User-Equipment-Info-Value	M	This field contains the user MAC.
Proxy-Info	O <sub>C</sub>	This field contains information of the host.
Proxy-Host	M	This field contains the identity of the host that added the Proxy-Info field.
Proxy-State	M	This field contains state local information.
Route-Record	O <sub>C</sub>	This field contains an identifier inserted by a relaying or proxying node to identify the node it received the message from.
Service-Information	O <sub>M</sub>	This parameter holds the individual service specific parameters.
WiMAX-Information	O <sub>C</sub>	This parameter holds the WiMAX specific parameters.
R3-OC-Session-Continue	O <sub>M</sub>	
Old-Session-Id	O <sub>C</sub>	Included if initial Credit Request corresponds to an existing session.

Hotlining-Capabilities	O <sub>C</sub>	
Framed-IP-Address	O <sub>C</sub>	The IPv4 address allocated for the user
Framed-IPv6-Prefix	O <sub>C</sub>	The IPv6 address prefix allocated for the user.
Access-Network-Charging-Identifier-Gx	O <sub>C</sub>	
<del>AF-Charging-Identifier</del>	<del>O<sub>C</sub></del>	Only used in case of PCC. See [3] for further details.
Offline-Charging	O <sub>C</sub>	
AVP	O <sub>C</sub>	

1 Note: See TS32.240-720 [100] for the meaning of "OM" and "OC".

#### 2 **5.5.1.5.4 Credit-Control-Answer message**

3 The Credit-Control-Answer message (CCA) is indicated by the command-code field being set to 272 and the 'R' bit  
4 being cleared in the Command Flags field. It is used between the credit-control server and the Diameter credit-  
5 control client to acknowledge a Credit-Control-Request command.

6 Message format:

```
<CCA> ::= < Diameter Header: 272, PXY >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { Auth-Application-Id }
    { CC-Request-Type }
    { CC-Request-Number }
    [ User-Name ]
    [ CC-Session-Failover ]
    [ CC-Sub-Session-Id ]
    [ Acct-Multi-Session-Id ]
    [ Origin-State-Id ]
    [ Event-Timestamp ]
    [ Granted-Service-Unit ]
    * [ Multiple-Services-Credit-Control ]
    [ Cost-Information ]
    [ Final-Unit-Indication ]
    [ Check-Balance-Result ]
    [ Credit-Control-Failure-Handling ]
    [ Direct-Debiting-Failure-Handling ]
    [ Validity-time ]
    * [ Redirect-Host ]
    [ Redirect-Host-Usage ]
```

- [ Redirect-Max-Cache-Time ]
- \* [ Proxy-Info ]
- \* [ Route-Record ]
- \* [ Failed-AVP ]
- [ Service-Information ]
- \* [ AVP ]

Table 5-39 illustrates the basic structure of a Diameter Credit-Control-Answer message as used for online charging.

**Table 5-39 – Credit-Control-Answer Message Content**

AVP	Category	Description
Session-Id	M	This field identifies the operation session.
Result-Code	M	This field contains the result of the specific query.
Origin-Host	M	This field contains the identification of the source point of the operation and the realm of the operation originator.
Origin-Realm	M	This field contains the realm of the operation originator.
Auth-Application-Id	M	The field corresponds to the application ID of the Diameter Credit Control Application and is defined with the value 4.
CC-Request-Type	M	This field defines the transfer type: initial, update, terminate for session based charging and event for event based charging.
CC-Request-Number	M	This field contains the sequence number of the transferred messages.
User-Name	-	Not used in WiMAX.
CC-Session Failover	O <sub>C</sub>	This field contains an indication to the CTF whether or not a failover handling is to be used when necessary.
CC-Sub-session-Id	-	Not used in WiMAX.
Acct-Multi-Session-Id	-	Not used in WiMAX.
Origin-State-Id	-	Not used in WiMAX.
Event-Timestamp	-	Not used in WiMAX.
Granted-Service-Unit	-	Not used in WiMAX, see Multiple-Services-Credit-Control.
Tariff-Time-Change	-	
CC-Time	-	
CC-Money	-	

AVP	Category	Description
Unit-Value	-	
Value-Digits	-	
Exponent	-	
Currency-Code	-	
CC-Total-Octets	-	
CC-Input-Octets	-	
CC-Output-Octets	-	
CC-Service-Specific-Units	-	
AVP	-	
Multiple-Services-Credit-Control	O <sub>C</sub>	This field contains all parameters for the CTF quota management and defines the quotas to allow traffic to flow.
Granted-Service-Unit	O <sub>C</sub>	This field contains the amount of granted service units for a particular category.
Tariff-Time-Change	O <sub>C</sub>	This field identifies the reporting period for the granted service units, i.e. before, after or during tariff change.
CC-Time	O <sub>C</sub>	This field contains the amount of granted time.
CC-Money	-	Not used in WiMAX.
Unit-Value	-	
Value-Digits	-	
Exponent	-	
Currency-Code	-	
CC-Total-Octets	O <sub>C</sub>	This field contains the amount for sent and received octets.
CC-Input-Octets	O <sub>C</sub>	This field contains the amount for received octets.
CC-Output-Octets	O <sub>C</sub>	This field contains the amount for sent octets.
CC-Service-Specific-Units	O <sub>C</sub>	This field contains the amount for service specific units, e.g. number of events.
AVP	-	
Requested-Service-Unit	-	Not used in CCA.
Tariff-Time-Change	-	
CC-Time	-	
CC-Money	-	
Unit-Value	-	
Value-Digits	-	
Exponent	-	

AVP	Category	Description
Currency-Code	-	
CC-Total-Octets	-	
CC-Input-Octets	-	
CC-Output-Octets	-	
CC-Service-Specific-Units	-	
Used-Service-Unit	-	Not used in CCA.
Tariff-Time-Change	-	
CC-Time	-	
CC-Money	-	
Unit-Value	-	
Value-Digits	-	
Exponent	-	
Currency-Code	-	
CC-Total-Octets	-	
CC-Input-Octets	-	
CC-Output-Octets	-	
CC-Service-Specific-Units	-	
Tariff-Change-Usage	O <sub>C</sub>	This field identifies the reporting period for the used service unit, i.e. before, after or during tariff change.
Service-Identifier	O <sub>C</sub>	This field contains identity of the used service. This ID with the Service-Context-ID together forms a unique identification of the service.
Rating-Group	O <sub>C</sub>	This field contains the identifier of a rating group.
G-S-U-Pool-Reference	O <sub>C</sub>	Only used in ECUR and SCUR.
G-S-U-Pool-Identifier	M	This field identifies a credit pool within the session.
CC-Unit-Type	M	This field specifies the type of units considered to be pooled into a credit pool.
Unit-Value	M	Used as defined in [63].
Value-Digits	M	Used as defined in [63].
Exponent	O <sub>C</sub>	Used as defined in [63].
Validity-Time	O <sub>C</sub>	This field defines the time in order to limit the validity of the granted quota for a given category instance.
Result-Code	O <sub>C</sub>	This field contains the result of the query.
Final-Unit-Indication	O <sub>C</sub>	This field indicates that the Granted-Service-Unit containing the final units for the service.
Final-Unit-Action	O <sub>C</sub>	This field indicates to the credit-control client the action to be taken when the user's account cannot



AVP	Category	Description
		cover the service cost.
Restriction-Filter-Rule	O <sub>C</sub>	This field provides filter rules corresponding to services that are to remain accessible even if there are no more service units granted.
Filter-Id	O <sub>C</sub>	This field contains the name of the filter list for this user.
Redirect-Server	O <sub>C</sub>	This field contains the address information of the redirect server.
Redirect-Address-Type	M	This field defines the address type of the address given in the Redirect-Server-Address AVP.
Redirect-Server-Address	M	This field defines the address of the redirect server.
Time-Quota-Threshold	O <sub>C</sub>	
Volume-Quota-Threshold	O <sub>C</sub>	Used as defined in [99].
Unit-Quota-Threshold	O <sub>C</sub>	Used as defined in [99].
Quota-Holding-Time	O <sub>C</sub>	
Quota-Consumption-Time	O <sub>C</sub>	
Trigger	O <sub>C</sub>	Used as defined in [99].
Trigger-Type	O <sub>C</sub>	Used as defined in [99].
AVP	-	
Cost-Information	O <sub>C</sub>	Used as defined in [63].
Unit-Value	M	Used as defined in [63].
Value-Digits	M	Used as defined in [63].
Exponent	O <sub>C</sub>	Used as defined in [63].
Currency-Code	M	Used as defined in [63].
Cost-Unit	O <sub>C</sub>	Used as defined in [63].
Low-Balance-Indication	O <sub>C</sub>	This field indicates whether the subscriber account balance went below a designated threshold set by his account.
Remaining-Balance	O <sub>C</sub>	This field contains the remaining balance of the subscriber.
Unit-Value	M	Used as defined in [63].
Value-Digits	M	Used as defined in [63].
Exponent	O <sub>C</sub>	Used as defined in [63].
Currency-Code	M	Used as defined in [63].
Final-Unit-Indication	-	Not used in WiMAX.
Final-Unit-Action	-	
Restriction-Filter-Rule	-	

AVP	Category	Description
Filter-Id	-	
Redirect-Server	-	
Redirect-Address-Type	-	
Redirect-Server-Address	-	
Check-Balance-Result	O <sub>C</sub>	This field contains the balance checking result.
Credit-Control-Failure-Handling	O <sub>C</sub>	Used as defined in [63].
Direct-Debiting-Failure-Handling	O <sub>C</sub>	Used as defined in [63].
Validity-Time	-	Not used in WiMAX.
Redirect-Host	O <sub>C</sub>	This field defines the time in order to limit the validity of the granted quota for a given category instance.
Redirect-Host-Usage	O <sub>C</sub>	Used as defined in [54].
Redirect-Max-Cache-Time	O <sub>C</sub>	Used as defined in [54].
Proxy-Info	O <sub>C</sub>	This field contains information of the host.
Proxy-Host	M	This field contains the identity of the host that added the Proxy-Info field.
Proxy-State	M	This field contains state local information.
Route-Record	O <sub>C</sub>	This field contains an identifier inserted by a relaying or proxying node to identify the node it received the message from.
Failed-AVP	O <sub>C</sub>	
Service-Information	O <sub>C</sub>	This parameter holds the individual service specific parameters.
WiMAX-Information	O <sub>C</sub>	This parameter holds the WiMAX specific parameters.
R3-OC-Session-Continue	O <sub>M</sub>	
AVP	O <sub>C</sub>	

Note: See TS32.240-720 [100] for the meaning of "OM" and "OC".

#### 5.5.1.5.5 R3-OC specific AVPs

R3-OC is based on RFC4006 [63]. It uses a part of RFC4006 AVPs (base Diameter and Diameter applications), that are identified for All Access Types. R3-OC additionally uses the optional R3-OC specific AVPs defined here and listed in Table 5-40.

**Table 5-40 –R3-OC specific AVPs**

Attribute Name	AVP Flag rules (note 1)				
	AVP Code	Clause defined	Value Type (note 2)	Must	Must not

R3-OC-Session-Continue	416	5.5.2.165	Enumerated	M,V	
Old-Session-Id	406	5.5.2.166	Integer32	M,V	
Service-Information	873	5.5.3.10	Grouped	M,V	
WiMAX-Information	409	5.5.2.167	Grouped	M,V	
NOTE 1: The AVP header bit denoted as 'M' indicates whether support of the AVP is required. The AVP header bit denoted as 'V' indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see RFC 3588 [54].					
NOTE 2: The value types are defined in RFC 3588 [54].					

#### 5.5.1.5.6 R3-OC Re-Used AVPs of external organizations

Table 5-41 lists the Diameter AVPs re-used by R3-OC interface from RFC4006 [63] and TS32.299 [99]. The other reused AVPs from the Diameter base protocol are not listed in Table 5-41.

**Table 5-41 –R3-OC re-used Diameter AVPs**

AVP	Reference	Description	Msg. Type
Access-Network-Charging-Identifier-Gx	[98]	Contains a charging identifier (PDFID for WiMAX) within the Access-Network-Charging-Identifier-Value AVP and the related PCC rule name(s) within the Charging-Rule-Name AVP(s).	CCR
Auth-Application-Id	[54]	This field identifies the Diameter Online application.	Both
CC-Input-Octets	[63]	This field contains the requested amount of octets to be received.	Both
CC-Output-Octets	[63]	This field contains the requested amount of octets to be sent.	Both
CC-Request-Type	[63]	This field defines the transfer type: event for event based charging and initial, update, terminate for session based charging.	Both
CC-Request-Number	[63]	This field contains the sequence number of the transferred messages.	Both
CC-Session-Failover	[63]	This field indicates if failover is supported.	CCA
CC-Service-Specific-Units	[63]	This field contains the requested amount of service specific units, e.g. number of events.	Both
CC-Time	[63]	This field contains the amount of requested time.	Both
CC-Total-Octets	[63]	This field contains the requested amount of octets to be sent and received.	Both
CC-Unit-Type	[63]	This field contains the type of units considered to be pooled.	CCA
Check-Balance-Result	[63]	This field contains the balance checking result.	CCA
Credit-Control-Failure-Handling	[63]	This field identifies what to do if sending credit-control messages to the credit-control server has been, for instance, temporarily prevented due to a network problem.	CCA
Cost-Information	[63]	This field contains the cost information of a service, which the credit-control client can transfer transparently to the end user.	CCA

Cost-Unit	[63]	This field contains the unit of the Cost-Information as human readable string.	CCA
Currency-Code	[63]	This field identifies the currency.	CCA
Destination-Host	[54]	This field contains the destination peer address of the OCS identity.	CCR
Direct-Debiting-Failure-Handling	[63]	This field identifies what to do if sending credit-control messages to the credit-control server has been, for instance, temporarily prevented due to a network problem.	CCA
Event-Timestamp	[54]	This field corresponds to the exact time the quota is requested	CCR
Exponent	[63]	This field contains the exponent value to be applied to Value-Digit-AVP.	CCA
Filter-Id	[62]	This field contains the name of the filter list for this user.	CCA
Final-Unit-Action	[63]	This field indicates to the credit-control client the action to be taken when the user's account cannot cover the service cost.	CCA
Final-Unit-Indication	[63]	This field indicates that the Granted-Service-Unit containing the final units for the service.	CCA
Framed-IP-Address	[63]	The IPv4 address allocated for the user	Both
Framed-IPv6-Prefix	[63]	The IPv6 address prefix allocated for the user.  The encoding of the value within this Octet String type AVP SHALL be as defined in [45], Clause 2.3. The "Reserved", "Prefix-Length" and "Prefix" fields SHALL be included in this order.	Both
Granted-Service-Unit	[63]	This field contains the amount of granted service units for a particular category.	CCA
G-S-U-Pool-Identifier	[99]	This field identifies a credit pool within the session.	CCA
G-S-U-Pool-Reference	[63]	This field contains the amount of granted service units for a particular category.	CCA
Low-Balance-Indication		This field indicates whether the subscriber account balance went below a designated threshold set by his account.	CCA
Multiple-Services-Credit Control	5.5.3.8	This field contains all parameters for the CTF quota management and defines the quotas to allow traffic to flow.	Both
Multiple-Services-Indicator	[63]	This field indicates whether the CTF is capable of handling multiple services independently.	Both
Offline-Charging	[99]	This field contains a reference to the Offline Charging.	CCR
Origin-Host	[54]	This field identifies the endpoint of the originated Diameter message.	Both
Origin-Realm	[54]	This field contains the Realm of the originator of any Diameter message.	Both
Origin-State-Id	[54]		CCR
Proxy-Host	[54]	This field contains the identity of the host that added the Proxy-Info.	Both
Proxy-Info	[54]		Both
Proxy-State	[54]	This field contains local state information.	Both
Quota-Consumption-Time	[99]	This field contains an idle traffic threshold time in seconds.	CCA
Quota-Holding-Time	[99]	This field contains the quota holding time in seconds.	CCA
Rating-Group	[63]	This field contains the identifier of a rating group.	Both

Redirect-Address-Type	[63]	This field defines the address type of the address given in the Redirect-Server-Address field.	CCA
Redirect-Host	[54]	This field identifies the host where the message should be forwarded to.	CCA
Redirect-Host-Usage	[54]	This field dictates how the routing entry resulting from the Redirect-Host is to be used.	CCA
Redirect-Max-Cache-Time	[54]	This field contains the maximum number of seconds the peer and route table entries.	CCA
Redirect-Server	[63]	This field contains the address information of the redirect server.	CCA
Redirect-Server-Address	[63]	This field defines the address of the redirect server.	CCA
Remaining-Balance		This field contains the remaining balance of the subscriber.	CCA
Reporting-Reason	[99]	This field specifies the reason for usage reporting for one or more types of quota for a particular category.	CCR
Requested-Action	[63]	The field defines the type of action if the CC-Request-Type indicates EVENT.	CCR
Requested-Service-Unit	[63]	This field contains the amount of requested service units for a particular category or an indication that units are needed for a particular category, as defined in [63].	CCR
Restriction-Filter-Rule	[63]	This field provides filter rules corresponding to services that are to remain accessible.	CCA
Result-Code	[63]	This field contains the result of the query.	CCA
Route-Record	[54]		Both
Service-Context-Id	[63]	This field contains a unique identifier of the Diameter credit-control service specific document that applies to the request.	CCR
Service-Identifier	[63]	This field contains identity of the used service. This ID with the Service-Context-ID together forms a unique identification of the service.	Both
Session-Id	[54]	This field is used to identify a specific session.	Both
Subscription-Id	[63]	This field contains the identification of the user that is going to access the service in order to be identified by the OCS.	CCR
Subscription-Id-Data	[63]	This field contains the user data content e.g. NAI for WiMAX.	CCR
Subscription-Id-Type	[63]	This field determines the type of the identifier, e.g. END_USER_NAI for WiMAX.	CCR
Tariff-Change-Usage	[63]	This field identifies the reporting period for the used service unit, i.e. before, after or during tariff change.	Both
Tariff-Time-Change	[63]	This field identifies the reporting period for the granted service units, i.e. before, after or during tariff change.	CCA
Termination-Cause	[54]	This field indicate the reason why a session was terminated.	CCR
Time-Quota-Mechanism	[99]		CCR
Time-Quota-Threshold	[99]	This field contains a threshold value in seconds.	CCA
Time-Quota-Type	[99]	This field indicate which time quota consumption mechanism SHALL be used for the associated Rating Group.	Both
Trigger	[99]	This field contains Trigger-Type.	Both

Trigger-Type	[99]	This field is used to negotiate triggers and when associated quota need to be re-authorised.	Both
Unit-Quota-Threshold	[99]	This field contains a threshold value in service specific units.	CCA
Unit-Value	[63]	This field specifies the units as decimal value.	CCA
User-Equipment-Info	[63]	This field contains the identification of the identity and terminal capability the subscriber is using for the connection to mobile network if available.	Both
User-Equipment-Info-Type	[63]	This field determines the type of the identifier.	CCR
User-Equipment-Info-Value	[63]	This field contains the user MAC.	CCR
User-Name	[54]	This field contains the User-Name, in a format consistent with the NAI specification.	CCR
Used-Service-Unit	[63]	This field contains the amount of used non-monetary service units measured for a particular category to a particular quota type.	CCR
Value-Digits	[63]	This field contains the significant digits of the number.	CCA
Validity-Time	[63]	This field defines the time in order to limit the validity of the granted quota for a given category instance.	CCA
Volume-Quota-Threshold	[99]	This field contains a threshold value in octets.	CCA

#### 5.5.1.5.7 Mobility handling

The procedure for mobility handling is in the scope of R3-OC specification [chapter 4.4.3.3.6]. In this procedure, the PPS can have two different modes upon PPC relocation,

- To continue with existing Pre-Paid context; or
- To start a new Pre-Paid session.

The mobility handling is subject to the following requirements:

- With WiMAX mobility handling specific AVP of R3-OC-Session-Continue , PPC needs to notify PPS that this CCR message is triggered by relocation, and PPS will decide which mode to use;
- For the initial CCR message with R3-OC-Session-Continue AVP, PPS needs to return a CCA message without granted credits information to PPC, and indicate to continue existing Pre-Paid context with R3-OC-Session-Continue AVP if PPS is pre-configured to support session continuity for mobility handling; otherwise,
- PPS just ignores the R3-OC-Session-Continue AVP in initial CCR message, and returns CCA message with granted credits information of an initial Pre-paid session to PPC. The client is advised to create a new session.
- Before relocation, if the pre-paid context is continued on new PPC, the old PPC sends termination CCR without consumption to PPS.

#### 5.5.1.6 Offline Accounting

Accounting Messages over PCC-R3-OFC Reference Point

##### 5.5.1.6.1 Accounting-Request Message

Diameter Accounting-Request message over the PCC-R3-OFC is defined as follows.

It can be used for the IP session based or PD flow based charging as well as for the PCC based charging.

<AC-Request> ::= < Diameter Header: 271, REQ, PXY >

< Session-Id >  
{ Origin-Host }  
{ Origin-Realm }  
{ Destination-Realm }  
{ Accounting-Record-Type }  
{ Accounting-Record-Number }  
[ Acct-Application-Id ]  
[ User-Name ]  
[ Acct-Session-Id ]  
[ Acct-Multi-Session-Id ]  
[ Origin-State-Id ]  
[ Destination-Host ]  
[ Event-Timestamp ]  
[ Acct-Delay-Time ]  
[ NAS-Identifier ]  
[ NAS-IP-Address ]  
[ NAS-IPv6-Address ]  
[ NAS-Port-Type ]  
\* [ Operator-Name ]  
\* [ Class ]  
[ Termination-Cause ]  
[ Accounting-Input-Octets ]  
[ Accounting-Input-Packets ]  
[ Accounting-Output-Octets ]  
[ Accounting-Output-Packets ]  
[ Acct-Link-Count ]  
[ Acct-Session-Time ]  
[ Calling-Station-Id ]  
[ Accounting-Realtime-Required ]  
[ Acct-Interim-Interval ]  
[ Framed-IP-Address ]  
[ Framed-IPv6-Prefix ]  
[ Framed-Interface-Id ]  
[ CUI ]  
\* [ Proxy-Info ]  
\* [ Route-Record ]

[ Session-Continue ]  
[ Beginning-Of-Session ]  
[ IP-Technology ]  
[ Hotline-Indication ]  
[ Prepaid-Indicator ]  
[ Idle-Mode-Transition ]  
[ Count-Type ]  
[ SDFID ]  
[ PDFID ]  
[ hHA-IP-MIP4 ]  
[ hHA-IP-MIP6 ]  
[ NAP-ID ]  
[ NSP-ID ]  
[ BS-ID ]  
[ Location ]  
[ GMT-Time-Zone-Offset ]  
[ Active-Time ]  
[ Control-Packets-In ]  
[ Control-Packets-Out ]  
[ Control-Octets-In ]  
[ Control-Octets-Out ]  
\* [ Uplink-Flow-Description ]  
\* [ Downlink-Flow-Description ]  
[ Uplink-Granted-QoS ]  
[ Downlink-Granted-QoS ]  
[ Visited-Framed-IP-Address ]  
[ Visited-Framed-Ipv6-Prefix ]  
[ Visited-Framed-Interface-Id ]  
[ Direction ]  
[ Interim-Cause ]

~~[ WiMAX QoS Information ]~~

Only used in case of PCC. See [3] for further details.

~~[ AF Correlation Information ]~~

Only used in case of PCC. See [3] for further details.

~~[ Charging Information ]~~

Only used in case of PCC. See [3] for further details.

\* [ AVP ]



#### 5.5.1.6.2 Accounting-Answer Message

Diameter Accounting-Answer message over the PCC-R3-OFC is defined as follows.

It can be used for the IP session based or PD flow based charging as well as for the PCC based charging.

<AC-Answer> ::= < Diameter Header: 271, PXY >

```
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { Accounting-Record-Type }
    { Accounting-Record-Number }
    [ Acct-Application-Id ]
    [ User-Name ]
    [ Acct-Session-Id ]
    [ Acct-Multi-Session-Id ]
    [ Event-Timestamp ]
    [ Error-Message ]
    [ Error-Reporting-Host ]
    * [ Failed-AVP ]
    [ Origin-State-Id ]
    [ Termination-Cause ]
    [ Accounting-Realtime-Required ]
    [ Acct-Interim-Interval ]
    * [ Class ]
    * [ Proxy-Info ]
    * [ Route-Record ]
    * [ AVP ]
```

```
<AC-Answer> ::= < Diameter Header: 271, PXY >
    < Session-Id >
    { Result-Code }
    { Origin-Host }
    { Origin-Realm }
    { Accounting-Record-Type }
    { Accounting-Record-Number }
    [ Acct-Application-Id ]
    [ User-Name ]
    [ Acct-Session-Id ]
    [ Acct-Multi-Session-Id ]
    [ Event-Timestamp ]
    [ Error-Message ]
    [ Error-Reporting-Host ]
    * [ Failed-AVP ]
```

```
[ Origin-State-Id ]
[ Termination-Cause ]
[ Accounting-Realtime-Required ]
[ Acct-Interim-Interval ]
* [ Class ]
* [ Proxy-Info ]
* [ Route-Record ]
* [ AVP ]
```

### 5.5.1.6.3 Overview of Diameter AVPs used for PCC-R3-OFC Reference points

If not differently mentioned, AVPs can be used in all kinds of WiMAX offline charging, including IP session based, PD flow based, and PCC based charging. All AVPs which are referenced in this section are allowed to be used for any kind of offline charging as far as there is no explicit restriction mentioned in this section or at the description of the AVP.

Table 5-42 provides the list of IETF Reused AVPs.

**Table 5-42 – IETF Reused AVPs**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Session-Id	263	UTF8String	RFC 3588	M	V
Origin-Host	264	DiamIdentity	RFC 3588	M	V
Origin-Realm	296	DiamIdentity	RFC 3588	M	V
Destination-Realm	283	DiamIdentity	RFC 3588	M	V
Accounting-Record-Type	480	Enumerated	RFC 3588	M	V
Accounting-Record-Number	485	Unsigned32	RFC 3588	M	V
Acct-Application-Id	259	Unsigned32	RFC 3588	M	V
User-Name	1	UTF8String	RFC 3588	M	V
Acct-Session-Id	44	OctetString	RFC 3588	M	V
Acct-Multi-Session-Id	50	Unsigned32	RFC 3588	M	V
Origin-State-Id	278	Unsigned32	RFC 3588	M	V
Destination-Host	293	DiamIdentity	RFC 3588	M	V
Event-Timestamp	55	Time	RFC 3588	M	V
Acct-Delay-Time	41	Unsigned32	RFC 4005	M	V
NAS-Identifier	32	UTF8String	RFC 4005	M	V
NAS-IP-Address	4	OctetString	RFC 4005	M	V
NAS-IPv6-Address	95	OctetString	RFC 4005	M	V
NAS-Port-Type	61	Enumerated	RFC 4005	M	V
Class	25	OctetString	RFC 3588	M	V
Termination-Cause	295	Enumerated	RFC 3588	M	V
Accounting-Input-Octets	363	Unsigned64	RFC 4005	M	V

Accounting-Input-Packets	365	Unsigned64	RFC 4005	M	V
Accounting-Output-Octets	364	Unsigned64	RFC 4005	M	V
Accounting-Output-Packets	366	Unsigned64	RFC 4005	M	V
Acct-Link-Count	51	Unsigned32	RFC 4005	M	V
Acct-Session-Time	46	Unsigned32	RFC 4005	M	V
Calling-Station-Id	31	UTF8String	RFC 4005	M	V
Accounting-Realtime-Required	483	Enumerated	RFC 3588	M	V
Acct-Interim-Interval	85	Unsigned32	RFC 3588	M	V
Framed-IP-Address	8	OctetString	RFC 4005	M	V
Framed-Ipv6-Prefix	97	OctetString	RFC 4005	M	V
Framed-Interface-Id	96	Unsigned64	RFC 4005	M	V
Proxy-Info	284	Grouped	RFC 3588	M	P,V
Route-Record	282	DiamIdentity	RFC 3588	M	P,V
CUI	89	UTF8String	RFC 4372	M	V
Result-Code	268	Unsigned32	RFC 3588	M	V
Error-Message	281	UTF8String	RFC 3588	-	V,M
Error-Reporting-Host	294	DiamIdentity	RFC 3588	-	V,M
Failed-AVP	279	Grouped	RFC 3588	M	V
Service-Context-Id	461	UTF8String	RFC 4006	M	V
Operator-Name	TBD	UTF8String	[96]	M	V

3GPP reused AVPs are listed in Table 5-43.

**Table 5-43 – 3GPP Reused AVPs**

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Service-Information	873	Grouped	TS 32.299	V,M	-
Access-Network-Charging-Identifier-Value	503	OctetString	TS 29.214	V,M	-
Access-Network-Charging-Address	501	Address	TS 29.214	V,M	-

WiMAX specific AVPs are presented in Table 5-44.

**Table 5-44 – WiMAX Specific AVPs**

AVP Name	AVP	Value		AVP Flag rules
----------	-----	-------	--	----------------

	Code	Type	Reference	Must	Must not
Session-Continue	21	Enumerated	5.5.2.20	V,M	-
Beginning-of-Session	22	Enumerated	5.5.2.21	V,M	-
Network-Technology	23	Enumerated	5.5.2.22	V,M	-
Hotline-Indication	24	OctetString	5.5.2.23	V,M	-
Hotlining-Capabilities	303	Unsigned32	5.5.2.67	V,M	-
Prepaid-Indicator	25	Enumerated	5.5.2.24	V,M	-
Idle-Mode-Transition	44	Enumerated	5.5.2.38	V,M	-
Count-Type	59	Enumerated		V,M	-
SDFID	27	OctetString	5.5.2.26	V,M	-
PDFID	26	OctetString	5.5.2.25	V,M	-
hHA-IP-MIP4	6	Address	5.5.2.6	V,M	-
hHA-IP-MIP6	7	Address	5.5.2.7	V,M	-
NAP-ID	45	OctetString	5.5.2.39	V,M	-
NSP-ID	57	OctetString	5.5.2.51	V,M	-
BS-ID	46	OctetString	5.5.2.40	V,M	-
Location	47	OctetString	5.5.2.41	V,M	-
GMT-Time-Zone-Offset	3	Integer32	5.5.2.3	V,M	-
Active-Time	39	Unsigned64	5.5.2.33	V,M	-
Control-Packets-In	31	Unsigned64	5.5.2.29	V,M	-
Control-Packets-Out	33	Unsigned64	5.5.2.31	V,M	-
Control-Octets-In	32	Unsigned64	5.5.2.30	V,M	-
Control-Octets-Out	34	Unsigned64	5.5.2.32	V,M	-
Uplink-Flow-Description	50	IPFilterRule		V,M	-
Downlink-Flow-Description	62	IPFilterRule		V,M	-
Uplink-Granted-QoS	30	Grouped	5.5.2.168	V,M	-
Downlink-Granted-QoS	63	Grouped	5.5.2.169	V,M	-
QoS-ID	312	Unsigned32	5.5.2.76	V,M	-
Global-Service-Class-Name	313	UTF8String	5.5.2.77	V,M	-
Service-Class-Name	314	UTF8String	5.5.2.78	V,M	-
Schedule-Type	315	Enumerated	5.5.2.79	V,M	-
Traffic-Priority	316	Unsigned32	5.5.2.80	V,M	-
Maximum-Sustained-Traffic-Rate	317	Unsigned32	5.5.2.81	V,M	-
Minimum-Reserved-Traffic-Rate	318	Unsigned32	5.5.2.82	V,M	-
Maximum-Traffic-Burst	319	Unsigned32	5.5.2.83	V,M	-

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Tolerated-Jitter	320	Unsigned32	5.5.2.84	V,M	-
Maximum-Latency	321	Unsigned32	5.5.2.85	V,M	-
Reduced-Resources-Code	322	Enumerated	5.5.2.86	V,M	-
Media-Flow-Type	323	Enumerated	5.5.2.87	V,M	-
Unsolicited-Grant-Interval	325	Unsigned32	5.5.2.88	V,M	-
SDU-Size	326	Unsigned32	5.5.2.89	V,M	-
Unsolicited-Polling-Interval	327	Unsigned32	5.5.2.90	V,M	-
Media-Flow-Description-In-SDP-Format	324	OctetString	5.5.2.114	V,M	-
Transmission-Policy	412	OctetString	5.5.2.115	V,M	-
Trigger	1264	Grouped	[99]	V,M	-
Trigger-Type	870	Enumerated	[99]	V,M	-
Unit-Quota-Threshold	1226	Unsigned32	[99]	V,M	-
Visited-Framed-IP-Address	79	OctetString	5.5.2.60	V,M	-
Visited-Framed-Ipv6-Prefix	80	OctetString	5.5.2.61	V,M	-
Visited-Framed-Interface-Id	81	Unsigned64	5.5.2.62	V,M	-
Volume-Quota-Threshold	869	Unsigned32	[99]	V,M	-
Direction	306	Enumerated	5.5.2.119	V,M	-
Interim-Cause	413	Enumerated	5.5.2.170	V,M	-
WiMAX-Information	409	Grouped	5.5.2.167	V,M	-

#### 5.5.1.6.4 AVP Occurrence Table

Table 5-45 shows which AVPs are to be present and used in accounting messages between the accounting client and the AAA, according to each accounting mode.

**Table 5-45 – AVP Occurrence Table**

AVP Name	Accounting mode		Accounting-Request			Accounting-Answer		
	IP	PD flow	START	INTERIM	STOP	START	INTERIM	STOP
Session-Id	X	X	1	1	1	1	1	1
Origin-Host	X	X	1	1	1	1	1	1
Origin-Realm	X	X	1	1	1	1	1	1
Destination-Realm	X	X	1	1	1	0	0	0
Accounting-Record-Type	X	X	1	1	1	1	1	1

AVP Name	Accounting mode		Accounting-Request			Accounting-Answer		
	IP	PD flow	START	INTERIM	STOP	START	INTERIM	STOP
Accounting-Record-Number	X	X	1	1	1	1	1	1
Acct-Application-Id	X	X	1	1	1	1	1	1
User-Name	X	X	1	1	1	1	1	1
Acct-Session-Id	X	X	1	1	1	1	1	1
Acct-Multi-Session-Id	X	X	1	1	1	1	1	1
Origin-State-Id	X	X	0-1	0-1	0-1	0-1	0-1	0-1
Destination-Host	X	X	0-1	0-1	0-1	0	0	0
Event-Timestamp	X	X	1	1	1	0-1	0-1	0-1
Acct-Delay-Time	X	X	0-1	0-1	0-1	0	0	0
NAS-Identifier	X	X	0-1	0-1	0-1	0	0	0
NAS-IP-Address	X	X	0-1[1]	0-1[1]	0-1[1]	0	0	0
NAS-IPv6-Address	X	X	0-1[1]	0-1[1]	0-1[1]	0	0	0
NAS-Port-Type	X	X	0-1	0-1	0-1	0	0	0
Operator-Name	X	X	0-2[16]	0-2[16]	0-2[16]			
Class	X	X	0+[2]	0+[2]	0+[2]	0+	0+	0+
Termination-Cause	X	X	0	0	1	0	0	0-1
Accounting-Input-Octets	X	X	0	1	1	0	0	0
Accounting-Input-Packets	X	X	0	1	1	0	0	0
Accounting-Output-Octets	X	X	0	1	1	0	0	0
Accounting-Output-Packets	X	X	0	1	1	0	0	0
Acct-Link-Count	X	X	0-1	0-1	0-1	0	0	0
Acct-Session-Time	X	X	0	0-1	0-1	0	0	0
Calling-Station-Id	X	X	0-1	0-1	0-1	0	0	0
Accounting-Realtime-Required	X	X	0-1	0-1	0-1	0-1	0-1	0-1
Acct-Interim-Interval	X	X	0-1	0-1	0-1	0-1	0-1	0-1
Framed-IP-Address	X	X	0-1[3]	0-1[3]	0-1[3]	0	0	0
Framed-Ipv6-Prefix	X	X	0-1[3]	0-1[3]	0-1[3]	0	0	0
Framed-Interface-Id	X	X	0-1[3]	0-1[3]	0-1[3]	0	0	0
Visited-Framed-IP-Address	X	X	0-1	0-1	0-1	0	0	0
Visited-Framed-Ipv6-Prefix	X	X	0-1	0-1	0-1	0	0	0
Visited-Framed-Interface-Id	X	X	0-1	0-1	0-1	0	0	0
Proxy-Info	X	X	0+	0+	0+	0+	0+	0+

AVP Name	Accounting mode		Accounting-Request			Accounting-Answer		
	IP	PD flow	START	INTERIM	STOP	START	INTERIM	STOP
Route-Record	X	X	0+	0+	0+	0+	0+	0+
CUI	X	X	0-1[4]	0-1[4]	0-1[4]	0	0	0
Result-Code	X	X	0	0	0	1	1	1
Error-Message	X	X	0	0	0	0-1	0-1	0-1
Error-Reporting-Host	X	X	0	0	0	0-1	0-1	0-1
Failed-AVP	X	X	0	0	0	0-1	0-1	0-1
Session-Continue	X	X	0	0	0-1[5]	0	0	0
Beginning-of-Session	X	X	0-1[5]	0	0	0	0	0
IP-Technology	X	X	0-1[5]	0-1[5]	0-1[5]	0	0	0
Hotline-Indication	X	X	0-1[6]	0-1[6]	0-1[6]	0	0	0
Prepaid-Indicator	X	X	0-1	0-1	0-1	0	0	0
Idle-Mode-Transition	X	X	0	0-1[7]	0	0	0	0
Count-Type	X	X	0	0-1[8]	0-1[8]	0	0	0
hHA-IP-MIP4	X	X	0-1	0-1	0-1	0	0	0
hHA-IP-MIP6	X	X	0-1	0-1	0-1	0	0	0
NAP-ID	X	X	0-1[9]	0-1[9]	0-1[9]	0	0	0
BS-ID	X	X	0-1[9]	0-1[9]	0-1[9]	0	0	0
NSP-ID	X	X	0-1[10]	0-1[10]	0-1[10]	0	0	0
Location	X	X	0-1	0-1	0-1	0	0	0
GMT-Time-Zone-Offset	X	X	0-1	0-1	0-1	0	0	0
Active-Time	X	X	0	0-1[11]	0-1[11]	0	0	0
Control-Packets-In	X	X	0	0-1[11]	0-1[11]	0	0	0
Control-Packets-Out	X	X	0	0-1[11]	0-1[11]	0	0	0
Control-Octets-In	X	X	0	0-1[11]	0-1[11]	0	0	0
Control-Octets-Out	X	X	0	0-1[11]	0-1[11]	0	0	0
Interim-Cause	X	X	0	1	0	0	0	0
SDFID	-	X	0-1[12]	0-1[12]	0-1[12]	0	0	0
PDFID	-	X	0-1[13]	0-1[13]	0-1[13]	0	0	0
Uplink-Flow-Description	-	X	0	0+[14]	0+[14]	0	0	0
Downlink-Flow-Description	-	X	0	0+[14]	0+[14]	0	0	0
Uplink-Granted-QoS	-	X	0-1	0-1[15]	0-1[15]	0	0	0
Downlink-Granted-QoS	-	X	0-1	0-1[15]	0-1[15]	0	0	0

AVP Name	Accounting mode		Accounting-Request			Accounting-Answer		
	IP	PD flow	START	INTERIM	STOP	START	INTERIM	STOP
QoS-ID	-	X	0-1	0-1	0-1	0	0	0
Global-Service-Class-Name	-	X	0-1	0-1	0-1	0	0	0
Service-Class-Name	-	X	0-1	0-1	0-1	0	0	0
Schedule-Type	-	X	0-1	0-1	0-1	0	0	0
Traffic-Priority	-	X	0-1	0-1	0-1	0	0	0
Maximum-Sustained-Traffic-Rate	-	X	0-1	0-1	0-1	0	0	0
Minimum-Reserved-Traffic-Rate	-	X	0-1	0-1	0-1	0	0	0
Maximum-Traffic-Burst	-	X	0-1	0-1	0-1	0	0	0
Tolerated-Jitter	-	X	0-1	0-1	0-1	0	0	0
Maximum-Latency	-	X	0-1	0-1	0-1	0	0	0
Reduced-Resources-Code	-	X	0-1	0-1	0-1	0	0	0
Media-Flow-Type	-	X	0-1	0-1	0-1	0	0	0
Unsolicited-Grant Interval	-	X	0-1	0-1	0-1	0	0	0
SDU-Size	-	X	0-1	0-1	0-1	0	0	0
Unsolicited-Polling-Interval	-	X	0-1	0-1	0-1	0	0	0
Media-Flow-Description-In-SDP-Format	-	X	0-1	0-1	0-1	0	0	0
Transmission-Policy	-	X	0-1	0-1	0-1	0	0	0
Direction	-	X	0-1	0-1	0-1	0	0	0

1

## 2 Notes:

- [1] At least one of NAS-IP-Address or NAS-IPv6-Address SHALL appear in the Accounting message.
- [2] Class SHALL be included if received in the Diameter DEA command.
- [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 be included if received in the Diameter DEA command.
- [5] SHALL NOT be included if accounting is performed in a HA.
- [6] If the session is Hot-Lined, and the NAS received this in the Diameter DEA or WCAR message, then the NAS SHALL include this attribute as received in the Accounting messages.
- [7] Only included when supported by the NAS and Idle Mode Notification has been requested by the HAAA. Never appears in messages from the HA.
- [8] Included whenever counter information is supplied.
- [9] At least NAP-ID or BS-ID SHALL appear in the Accounting message. If both appear then the receiver SHALL ignore the NAP-ID attribute. These attribute SHALL not be inserted by a HA generating



accounting messages.

- [10] 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.
- [11] SHALL NOT be reported by a HA.
- [12] SHALL not be included when session based accounting. Included, if available, when flow-based accounting is used. SHALL NOT be reported by a HA.
- [13] SHALL be included when flow based accounting is being performed. SHALL not be included with Session-based accounting. SHALL NOT be reported by a HA.
- [14] Attribute SHALL not appear when Session-based accounting is performed.  
The MS's IP address (HoA) SHALL be included 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.
- [15] This attribute SHALL NOT be included in the case Session-based accounting has been activated or if accounting messages are sent by the Accounting Client in an HA.
- [16] The VNSP SHALL include the Operator-Name it included in the WDER command and the Operator-Name it received from the HAAA in the WDEA command.

1  
2

## 5.5.2 WiMAX DIAMETER VSAs Definitions

The following section defines the WiMAX Vendors specific AVPs.

Value types are as specified by RFC3588 [54]. Bit-Map types are as specified in the RADIUS section [5.4.2]

### 5.5.2.1 WiMAX-Capability

<b>WType-ID</b>	1 for WiMAX-Capability
<b>Description</b>	In a Request the AVP identifies the WiMAX Capabilities supported by the ASN or the HA. In an Answer, signals the options selected by the Diameter server.
<b>Value-Type</b>	Grouped
<b>Value</b>	

In a Request the AVP identifies the WiMAX Capabilities supported by the ASN or the HA. In an Answer, signals the options selected by the Diameter server.

WiMAX-Capability ::= < AVP Header: 1 >

```

    { WiMAX-Release}
    { Accounting-Capabilities }
    [ Hotlining-Capabilities ]
    [Idle-Mode-Notification-Capabilities]
    [Packet-Flow-Descriptor-Capabilities] (This TLV
    is deprecated in this release and SHALL not be
    used.)
    [Authorized-Network-Services]
    [ASN-Network-Service-Capabilities]
    [VCSN-Network-Service-Capabilities]
    [Visited-Authorized-Network-Services]
    [Mobility-Access-Capabilities]
    [ROHC-Support]
    [Release-Supported]
    [Version-Negotiation-Flag]
    *[AVP]

```

AVP	TLV Name	Request	Answer
301	WiMAX-Release	1	1
302	Accounting-Capabilities	1	1
303	Hotlining-Capabilities	0-1[a]	0

304	Idle-Mode-Notification-Capabilities	0-1[b]	0-1[c]
344	Packet-Flow-Descriptor-Capabilities	0-1[d]	0-1[d]
345	Authorized-Network-Services	0	0-1
346	ASN-Network-Service-Capabilities	1[e][g]	0
347	VCSN-Network-Service-Capabilities	0-1[f][g]	0
348	Visited-Authorized-Network-Services	0	1[g]
395	Mobility-Access-Capabilities	1	0
396	ROHC-Support	0-1[h]	0-1[i]
397	Release-Supported	0-1	0-1
398	Version-Negotiation-Flag	0-1	0-1

## Notes:

- [a] The absence of this AVP in a Request means that the NAS or HA does not support Hot-Lining.
- [b] The absence of this AVP in a Request means that the NAS does not support Idle Mode Notification. This AVP SHALL NOT appear in a Request originating from an HA. The HAAA SHALL silently ignore this AVP in messages originating from an HA.
- [c] The absence of this AVP in an Answer means that the HAAA does not require Idle Mode Notification. The HAAA SHALL NOT send this AVP to an HA. An HA SHALL silently ignore this AVP.
- [d] Not used. The usage of this TLV is deprecated, as support of Packet-Flow-Descriptor is deprecated in this release. Only Packet-Flow-Descriptor V2 SHALL be supported.
- [e] This AVP should be present when MS attaches through the visited network, included by the VCSN to indicate its supported network service capabilities.
- [f] This sub-TLV should be present when MS attaches through the visited network, included by the VCSN to indicate its supported network service capabilities.
- [g] This TLV SHALL NOT be included for any WiMAX Release prior to 1.5.
- [h] The absence of this sub-TLV in a Request (WDER) means that the ASN does not support ROHC.
- [i] The absence of this sub-TLV in an Answer (WDEA) message means that the HAAA does not require ROHC. The HAAA SHALL NOT send this sub-TLV to a HA. An HA SHALL silently ignore this sub-TLV.

### 5.5.2.2 Device-Authentication-Indicator

<b>WType-ID</b>	2 for Device-Authentication-Indicator
<b>Description</b>	This attribute is deprecated in RADIUS and DIAMETER and MUST NOT be used.
<b>Value-Type</b>	
<b>Value</b>	

### 5.5.2.3 GMT-Time-Zone-Offset

<b>WType-ID</b>	3 for GMT-Timezone-offset
<b>Description</b>	The current offset in seconds of the local time at the NAS with respect to GMT time.

<b>Value-Type</b>	Integer32
<b>Value</b>	Indicating a timeoffset in seconds.

1 **5.5.2.4 WiMAX-Session-Id**

<b>WType-ID</b>	4 for WiMAX-Session-Id
<b>Description</b>	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. A WiMAX session is established when the MS performs a successful initial network entry. The WiMAX session is terminated when network exit procedures are performed.
<b>Value-Type</b>	OctetString
<b>Value</b>	Octet String. The value of the WiMAX-Session-Id

2 **5.5.2.5 MSK**

<b>WType-ID</b>	5 for MSK
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT be used in Diameter. In Diameter use EAP-Master-Session-Key (464) AVP defined by RFC4072 to carry the resulting Master session key obtained after successfully executing EAP authentication.
<b>Value-Type</b>	OctetString
<b>Value</b>	Octet String. The value of the MSK.

3 **5.5.2.6 hHA-IP-MIP4**

<b>WType-ID</b>	6 for hHA-IP-MIP4
<b>Description</b>	The IPv4 address of the HA.
<b>Value-Type</b>	Address
<b>Value</b>	An IPv4 address as defined byRFC3588

4 **5.5.2.7 hHA-IP-MIP6**

<b>WType-ID</b>	7 for hHA-IP-MIP6
<b>Description</b>	The IPv6 address of the HA used for MIP6.
<b>Value-Type</b>	Address
<b>Value</b>	An IPv6 address as defined byRFC3588

5 **5.5.2.8 hDHCPv4-Server**

<b>WType-ID</b>	8 for DHCPv4-Server
<b>Description</b>	The IPv4 address of the DHCP-Server to use for IPv4 address allocation by the ASN.
<b>Value-Type</b>	Address
<b>Value</b>	IPv4 as defined by RFC3588

1 **5.5.2.9 hDHCPv6-Server**

<b>WType-ID</b>	9 for DHCPv6-Server
<b>Description</b>	The IPv6 address of the DHCP-Server to use for IPv6 allocation by the ASN.
<b>Value-Type</b>	Address
<b>Value</b>	IPv6 as defined by RFC3588

2 **5.5.2.10 MN-HA-MIP4-KEY**

<b>WType-ID</b>	10 for MN-HA-MIP4-KEY
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT to be used in Diameter. In Diameter use MN-HA-MIP4-MSA to transport the MN HA key.

3 **5.5.2.11 MN-HA-MIP4-SPI**

<b>WType-ID</b>	11 MN-HA-MIP4-SPI
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT to be used in Diameter. In Diameter use MIP-MN-HA-SPI (TBD) defined in SPLIT.

4 **5.5.2.12 MN-HA-MIP6-KEY**

<b>WType-ID</b>	12 for MN-HA-MIP6-KEY
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT to be used in Diameter. In Diameter use MN-HA-MIP6-MSA to transport the MN HA key for MIP6.

5 **5.5.2.13 MN-HA-MIP6-SPI**

<b>WType-ID</b>	13 MN-HA-MIP6-SPI
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT to be used in Diameter. In Diameter use MIP-MN-HA-SPI (TBD) defined in SPLIT.

6 **5.5.2.14 FA-RK-KEY**

<b>WType-ID</b>	14 for FA-RK-KEY
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT to be used in Diameter. In Diameter use FA-RK-MSA(330) to transport the FA-RK key.

7 **5.5.2.15 HA-RK-KEY**

<b>WType-ID</b>	15 for HA-RK-KEY
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT to be used in Diameter. In Diameter use HA-RK-MSA(331) to transport the HA-RK key.

8 **5.5.2.16 HA-RK-SPI**

<b>WType-ID</b>	16 for HA-RK-SPI
<b>Description</b>	The SPI used for the HA-RK.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	An unsigned value representing a SPI.

#### 5.5.2.17 HA-RK-Lifetime

<b>WType-ID</b>	17 for HA-RK-Lifetime
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT to be used in Diameter. In Diameter use HA-RK-MSA(331) to transport the HA-RK-Lifetime.

#### 5.5.2.18 RRQ-HA-IP

<b>WType-ID</b>	18 for RRQ-HA-IP
<b>Description</b>	The IPv4 or IPv6 address of the HA as contained in the MIP Registration Request or the BU.
<b>Value-Type</b>	Address
<b>Value</b>	Octet string containing an IPv4 or IPv6 address (most significant bit first)

#### 5.5.2.19 RRQ-MN-HA-KEY

<b>WType-ID</b>	19 for RRQ-MN-HA-KEY
<b>Description</b>	The MN_HA key sent by the AAA server to the HA to be used to validate the MN-HA-AE of the Mobile IP Registration Request.
<b>Value-Type</b>	OctetString
<b>Value</b>	The value consists of key most significant byte first.

#### 5.5.2.20 Session-Continue

**Note:** This AVP is referenced by the PCC specification [3].

<b>WType-ID</b>	21 for Session-Continue
<b>Description</b>	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.
<b>Value-Type</b>	Enumerated
<b>Value</b>	Allowed values: <ul style="list-style-type: none"> <li>False(0)</li> <li>True(1)</li> </ul> All other values reserved

#### 5.5.2.21 Beginning-of-Session

**Note:** This AVP is referenced by the PCC specification [3].

<b>WType-ID</b>	22 for Beginning-of-Session
<b>Description</b>	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.
<b>Value-Type</b>	Enumerated
<b>Value</b>	Allowed values: <ul style="list-style-type: none"> <li>False(0)</li> <li>True(1)</li> </ul> All other values reserved

### 5.5.2.22 Network-Technology

**Note: This AVP is referenced by the PCC specification [3].**

<b>WType-ID</b>	23 for Network-Technology
<b>Description</b>	This attribute indicates which type of WiMAX session is being used.
<b>Value-Type</b>	Enumerated
<b>Value</b>	The enumeration is defined as follows: <ul style="list-style-type: none"><li>• 0 = Simple IPv4</li><li>• 1 = Simple IPv6</li><li>• 2 = PMIP4</li><li>• 3 = CMIP4</li><li>• 4 = CMIP6</li><li>• 5 = Ethernet-CS</li><li>• 6 = Simple ETH</li><li>• 7 = MIP based ETH</li></ul> All other values reserved

### 5.5.2.23 Hotline-Indication

**Note: This AVP is referenced by the PCC specification [3].**

<b>WType-ID</b>	24 for Hotline-Indication
<b>Description</b>	This attribute in a AAA WACR command indicates to back-office systems (billing audit systems) that the session has been Hot-Lined. Exactly one of these AVP may appear in a AAA message. If the Hot-lining Device received this attribute from the AAA server, then it SHALL include the attribute in any subsequent AAA WACR command for that session.
<b>Value-Type</b>	UTF8String
<b>Value</b>	A string value which is to be opaque.

### 5.5.2.24 Prepaid-Indicator

**Note: This AVP is referenced by the PCC specification [3].**

<b>WType-ID</b>	25 for Prepaid-Indicator
<b>Description</b>	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.
<b>Value-Type</b>	Enumerated
<b>Value</b>	Allowed values: <ul style="list-style-type: none"><li>• Offline(0)</li><li>• Online(1)</li></ul> All other values reserved

### 5.5.2.25 PDFID

<b>WType-ID</b>	26 for PDFID
-----------------	--------------

<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Packet Data Flow Identifier. (Most significant bit first) less than $2^{16}$

#### 1 5.5.2.26 SDFID

<b>WType-ID</b>	27 for SDFID
<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Service Data Flow Identifier (Most significant bit first) less than $2^8$

#### 2 5.5.2.27 Packet-Flow-Descriptor<sup>35</sup> (This AVP is deprecated in this release)

#### 3 5.5.2.28 QoS-Descriptor

<b>Type-ID</b>	29 for QoS-Descriptor
<b>Description</b>	This attribute describes over the air QoS parameters that are associated with a flow.
<b>Value-Type</b>	Grouped

4

QoS-Descriptor ::= < AVP Header: 29 >

```

    { QoS-ID }
    { Schedule-Type }
    [ Global-Service-Class-Name ]
    [ Service-Class-Name ]
    [ Traffic-Priority ]
    [ Maximum-Sustained-Traffic-Rate ]
    [ Minimum-Reserved-Traffic-Rate ]
    [ Maximum-Traffic-Burst ]
    [ Tolerated-Jitter ]
    [ Maximum-Latency ]
    [ Reduced-Resource-Code ]
    [ Media-Flow-Type ]
    [ Unsolicited-Grant-Interval ]
    [ SDU-Size ]
    [ Unsolicited-Polling-Interval ]
    [ Media-Flow-Description-In-SDP-Format ]

```

<sup>35</sup> This Attribute SHALL not be used, as the support of Packet Flow Descriptor is deprecated in this release. Only Packet Flow Descriptor V2 SHALL be supported instead



[ Transmission-Policy ]

[DSCP]

\* [ AVP ]

The occurrence of the attributes in the QoS-Descriptor AVP is governed by the value of the Schedule-Type AVP.

TLV ID	TLV Name	Answer	Notes
312	QoS-ID	1	
315	Schedule-Type	1	
314	Service-Class-Name	0-1	
316	Traffic-Priority	0-1	See Table 5-46 If omitted the traffic priority is assumed to be 0.
317	Maximum-Sustained-Traffic-Rate	0-1	See Table 5-46
318	Minimum-Reserved-Traffic-Rate	0-1	See Table 5-46
319	Maximum-Traffic-Burst	0-1	See Table 5-46
320	Tolerated-Jitter	0-1	See Table 5-46
321	Maximum-Latency	0-1	See Table 5-46
322	Reduced-Resource-Code	0-1	See Table 5-46
323	Media-Flow-Type	0-1	See Table 5-46
325	Unsolicited-Grant-Interval	0-1	See Table 5-46
326	SDU-Size	0-1	See Table 5-46
327	Unsolicited-Polling-Interval	0-1	See Table 5-46
351	Media-Flow-Description-In-SDP-Format	0-1	
352	Transmission-Policy	0-1	If omitted the Transmission policy is assumed to be 0. If included, the ASN MAY ignore it
458	DSCP	0-1	

**Table 5-46 – Showing Valid QoS Attributes for Each Schedule-Type**

ID	QoS Parameter	BE	ERT-VR	UGS	RT-VR	NRT-VR
316	Traffic-Priority.	0-1[a]	0-1[a]	0	0-1[a]	0-1[a]

ID	QoS Parameter	BE	ERT-VR	UGS	RT-VR	NRT-VR
317	Maximum-Sustained-Traffic-Rate.	0-1	0-1 [b]	1	0-1[b]	0-1[b]
318	Minimum-Reserved-Traffic-Rate.	0	1	0-1[e]	1	1
319	Maximum-Traffic-Burst.	0	0-1	0	0-1	0-1
320	Tolerated-Jitter	0	0-1[c]	0-1[c]	0	0
321	Maximum-Latency.	0	1	1	1	0
325	Unsolicited-Grant-Interval	0	1	1	0	0
326	SDU-Size	0	0	0-1[d]	0	0
327	Unsolicited-Polling-Interval	0	0	0	1	0
352	Transmission-Policy	0-1[f]	0-1[f]	0-1[f]	0-1[f]	0-1[f]

1 **Notes:**

- [a] If omitted then traffic priority SHALL equal 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.
- [e] If present, it SHALL have the same value as the Maximum-Sustained-Traffic-Rate parameter.

2 **5.5.2.29 Control-Packets-In**

3 **Note: This AVP is referenced by the PCC specification [3].**

<b>WType-ID</b>	31 for Control-Packets-In
<b>Description</b>	Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.
<b>Value-Type</b>	6 + 3 + 4
<b>Value</b>	Unsigned Integer representing packets count.

4 **5.5.2.30 Control-Octets-In**

5 **Note: This AVP is referenced by the PCC specification [3].**

<b>WType-ID</b>	32 for Control-Octets-In
<b>Description</b>	Octet counts for incoming Mobile IPv4, DHCP, ICMP messages etc.
<b>Value-Type</b>	6 + 3 + 4
<b>Value</b>	Unsigned Integer representing octets.

### 5.5.2.31 Control-Packets-Out

**Note: This AVP is referenced by the PCC specification [3].**

<b>WType-ID</b>	33 for Control-Packets-Out
<b>Description</b>	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
<b>Value-Type</b>	6 + 3 + 4
<b>Value</b>	Unsigned Integer representing packets count.

### 5.5.2.32 Control-Octets-Out

**Note: This AVP is referenced by the PCC specification [3].**

<b>WType-ID</b>	34 for Control-Octets-Out
<b>Description</b>	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
<b>Value-Type</b>	6 + 3 + 4
<b>Value</b>	Unsigned Integer representing an octet count.

### 5.5.2.33 Active-Time

**Note: This AVP is referenced by the PCC specification [3].**

<b>WType-ID</b>	39 for Active-Time
<b>Description</b>	The amount of time the session was not in Idle state.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer. The time in seconds.

### 5.5.2.34 DHCP-RK

<b>WType-ID</b>	40 for DHCP-RK
<b>Description</b>	This attribute is defined in RADIUS and MUST NOT to be used in Diameter. In Diameter use DHCP-RK-SA(333) to transport the HA-RK key.
<b>Value-Type</b>	OctetString
<b>Value</b>	Key MSB first.

### 5.5.2.35 DHCP-RK-Key-ID

<b>WType-ID</b>	41 for DHCP-RK-Key-ID
<b>Description</b>	An integer number uniquely identifying the DHCP-RK within the scope of a single DHCP server.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	

### 5.5.2.36 DHCP-RK-Lifetime

<b>WType-ID</b>	42 for DHCP-RK-Lifetime
<b>Description</b>	Lifetime of the DHCP-RK and derived keys.

<b>Value-Type</b>	Unsigned32
<b>Value</b>	Representing the number of seconds the key is valid.

1 **5.5.2.37 DHCPMSG-Server-IP**

<b>WType-ID</b>	43 for DHCPMSG-Server-IP
<b>Description</b>	The IPv4 address of the DHCP server contained in the DHCPDISCOVER message.
<b>Value-Type</b>	Address
<b>Value</b>	Octet string containing an IPv4 address of DHCP server (most significant bit first) to which the DHCPDISCOVER/DHCPREQUEST message was sent.

2 **5.5.2.38 Idle-Mode-Transition**

<b>WType-ID</b>	44 for Idle-Mode-Transition
<b>Description</b>	A flag indicating whether the mobile node is in idle or not.
<b>Value-Type</b>	Enumerated
<b>Value</b>	Valid values: <ul style="list-style-type: none"> <li>• Active Mode (0)</li> <li>• Idle Mode (1)</li> </ul> All other values reserved.

3 **5.5.2.39 NAP-ID**

<b>WType-ID</b>	45 for NAP-ID
<b>Description</b>	Uniquely identifies the Network Access Provider.
<b>Value-Type</b>	OctetString
<b>Value</b>	Three octets representing an operator identifier.

4 **5.5.2.40 BS-ID**

<b>WType-ID</b>	46 for BS-ID
<b>Description</b>	Uniquely identifies a NAP and a Base Station within that NAP.
<b>Value-Type</b>	OctetString
<b>Value</b>	6 Octet-String. Representing NAP operator identifier (first 3 Octets) and the Base Station ID (next 3 Octets)

5 **5.5.2.41 Location**

<b>WType-ID</b>	47 for Location
<b>Description</b>	Location of the ASN.
<b>Value-Type</b>	UTF8String
<b>Value</b>	Octet-String representing location. Format is TBD

#### 5.5.2.42 Acct-Input-Packets-Gigaword

#### 5.5.2.43 Acct-Output-Packets Gigaword

#### 5.5.2.44 Flow-Description

<b>WType-ID</b>	50 for Flow-Description
<b>Description</b>	Describes a flow classifier.
<b>Value-Type</b>	Classifier
<b>Value</b>	

#### 5.5.2.45 BU-CoA-Ipv6

<b>WType-ID</b>	51 for BU-CoA-IPv6
<b>Description</b>	The CoA from the BU message.
<b>Value-Type</b>	Address
<b>Value</b>	Octet-String representing an IPv6 address as per RFC3588

#### 5.5.2.46 DNS

<b>WType-ID</b>	52 for DNS
<b>Description</b>	The IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.
<b>Value-Type</b>	Address
<b>Value</b>	An IPv4 or IPv6 address as per RFC3588

#### 5.5.2.47 Hotline-Profile-ID

<b>WType-ID</b>	53 for Hotline-Profile-ID
<b>Description</b>	A unique identifier (relative to the HCSN) of a Hot-Line profile to be applied to this session.
<b>Value-Type</b>	UTF8String
<b>Value</b>	<p>UTF8 String representing a Hot-Line profile formatted as follows: realm + "/" + profile-id-string</p> <p>Where:</p> <ul style="list-style-type: none"> <li>• Realm is the Fully Qualified Domain Name of the operator that is asserting the Hotline profile; and</li> <li>• Profile-id-string is operator specific label for the hotline profile to be applied at the by the Hot-Lining device.</li> </ul>

#### 5.5.2.48 HTTP-Redirection-Rule

<b>WType-ID</b>	54 for HTTP-Redirection-Rule
<b>Description</b>	An HTTP redirection rule. When one or more of the classifier matches the NAS responds back with the specified URL causing the client's browser to be redirected to that URL.
<b>Value-Type</b>	Grouped

HTTP-Redirection-Rule::= < AVP Header: 54>

{ Redirection-Action }  
[ Redirect-URL ]                      The redirection URL.  
\* [ IP-Classifer ]                      The matching classifier  
\*[AVP]

1

AVP	TLV Name	Answer	Notes
335	Redirection-Action	1	
336	Redirect-URL	0-1	If HTTP-Redirection-Action is equal to “redirect” then this attribute MUST be included. Otherwise, this attribute MUST NOT be included. If the attribute is included the receiver MUST ignore this attribute.
311	IP-Classifer	0-n	If HTTP-Redirection-Action is equal to flush, the classifier MUST NOT be included. If included then the receiver MUST ignore the classifiers. If HTTP-Redirection-Action is set to “pass” or “redirect” then at least one Classifier MUST be included.  When multiple values of classifiers appear in the packet, processing proceeds in the order that the classifiers appear in the AVP until a classifier is matched.

2

### 3 5.5.2.49 IP-Redirection-Rule

<b>WType-ID</b>	55 for IP-Redirection-Rule
<b>Description</b>	An IP redirection rule. When one or more of the classifier matches the NAS rewrites the destination IP address and optionally port with the specified value.
<b>Value-Type</b>	Grouped

4

IP-Redirection-Rule ::= < AVP Header: 55>

{ IP-Redirection-Action }  
[ Redirect-Address ]                      The IP address to redirect matching packets  
  
[ Redirect-Port ]                      The Port to redirect packets to.  
\* [ IP-Classifer ]                      The matching classifier(s).  
\*[AVP]

5

AVP	TLV Name	Answer	Notes
335	Redirection-Action	1	
340	Redirect-Address	0-1	If HTTP-Redirection-Action is equal to “redirect” then this attribute MUST be included. Otherwise, this attribute MUST NOT be included. If the attribute is included the receiver MUST ignore this attribute. Value MUST be IPv4. Receiver MUST reject the command if the value is IPv6
341	Redirect-Port	0-1	If IP-Address is included then this attribute MAY be included, otherwise this attribute MUST NOT be included. The receiver MUST ignore this attribute if IP-Address AVP is not included
311	IP-Classifier	0-n	If HTTP-Redirection-Action is equal to flush, the classifier MUST NOT be included. If included then the receiver MUST ignore the classifiers. If HTTP-Redirection-Action is set to “pass” or “redirect” then at least one Classifier MUST be included. When multiple values of classifiers appear in the packet, processing proceeds in the order that the classifiers appear in the AVP until a classifier is matched.

1

## 2 5.5.2.50 Hotline-Session-Timer

<b>WType-ID</b>	56 for Hotline-Session-Timer
<b>Description</b>	The length of time in seconds the session can remain Hot-Lined. If not specified the length of time the session is Hot-Lined 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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Representing a time in seconds. A value of zero means infinity.

## 3 5.5.2.51 NSP-ID

<b>WType-ID</b>	57 for NSP-ID
<b>Description</b>	Uniquely identifies the Network Service Provider.
<b>Value-Type</b>	OctetString

<b>Value</b>	Octet-String (3 Octets) representing an operator identifier.
--------------	--

1 **5.5.2.52 HA-RK-Key-Requested**

2 Not used.

3 **5.5.2.53 Count-Type**

<b>WType-ID</b>	59 for Count-Type
<b>Description</b>	Used to indicate if the record represents compressed or uncompressed counts.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned32. When set to (0) indicates uncompressed counts. When set to (1) indicates compressed counts

4 **5.5.2.54 FA-RK-SPI**

<b>WType-ID</b>	61 for FA-RK-SPI
<b>Description</b>	The SPI used for the FA-RK.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Representing a SPI value.

5 **5.5.2.55 vHA-IP-MIP4**

<b>WType-ID</b>	64 for vHA-IP-MIP4
<b>Description</b>	The IPv4 address of the vHA for MIP4
<b>Value-Type</b>	Address
<b>Value</b>	An IPv4 address

6 **5.5.2.56 vHA-IP-MIP6**

<b>WType-ID</b>	65 for vHA-IP-MIP6
<b>Description</b>	The IPv6 address of the vHA for MIP6
<b>Value-Type</b>	Address
<b>Value</b>	An IPv6 address

7 **5.5.2.57 vDHCPv4-Server**

<b>WType-ID</b>	73 for vDHCPv4-Server
<b>Description</b>	The IPv4 or IPv6 address of the visited DHCP Server to use for IPv4 address allocation.
<b>Value-Type</b>	Address
<b>Value</b>	An IPv4 or IPv6 address

8 **5.5.2.58 vDHCPv6-Server**

<b>WType-ID</b>	74 for vDHCPv4-Server
<b>Description</b>	The IPv6 address of the visited DHCP Server to use for IPv6 address allocation.
<b>Value-Type</b>	Address



<b>Value</b>	An IPv6 address
--------------	-----------------

1 **5.5.2.59 PMIP-Authenticated-Network-Identity**

<b>WType-ID</b>	78 for PMIP-Authenticated-Network-Identity
<b>Description</b>	Identity of the MS to be used for PMIP operation as the NAI to be included in the PMIP NAI authentication extension.
<b>Value-Type</b>	UTF8String
<b>Value</b>	Contains an identity according to the NAI specification [RFC4282]

2 **5.5.2.60 Visited-Framed-IP-Address**

<b>WType-ID</b>	79 for Visited-Framed-IP-Address
<b>Description</b>	The IPv4 home address assigned by the Visited CSN to be used for the MS.
<b>Value-Type</b>	Address
<b>Value</b>	An IPv4 address

3 **5.5.2.61 Visited-Framed-IPv6-Address**

<b>WType-ID</b>	80 for Visited-Framed-IPv6-Address
<b>Description</b>	The IPv4 home address assigned by the Visited CSN to be used for the MS.
<b>Value-Type</b>	Address
<b>Value</b>	An IPv4 address

4 **5.5.2.62 Visited-Framed-Interface-Id**

<b>WType-ID</b>	81 for Visited-Framed-Interface-Id
<b>Description</b>	The IPv6 interface Id assigned by the Visited CSN to be used for the MS.
<b>Value-Type</b>	OctetString
<b>Value</b>	An IPv4 address

5 **5.5.2.63 Packet-Flow-Descriptor-V2**

<b>WType-ID</b>	84 for Packet-Flow-Descriptor-V2
<b>Description</b>	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.
<b>Value-Type</b>	Grouped

6

Packet-Flow-Descriptor-V2 ::= < AVP Header: 84>

{ PDFID }  
[ SDFID ]  
[ ServiceProfileID ]  
[ Direction ]

[ ActivationTrigger ]

[ Transport-Type ]

[ UplinkQoSID ]

Used to locate the QoS-Descriptor for uplink treatment

[ DownlinkQoSID ]

Used to locate the QoS-Descriptor for the downlink treatment

\* [ Classifier ]

Specifies the matching rules for this flow in the uplink or downlink direction.

[ Paging-Preference ]

[ VLANTagProcessingRuleID ]

\*[AVP]

1

TLV ID	TLV Name	Answer	Notes
26	PDFID	1	
27	SDFID	0-1	
305	ServiceProfileID	0-1	If ServiceProfileID is provided then TLV IDs greater than 3 overrides the QoS parameter settings of the related ServiceProfile according to the TLV-value. If ServiceProfileId or either of UplinkQoSID or DownlinkQoSID or IP-Classifier are missing then the NAS SHALL reject the network entry of the MS.
306	Direction	0-1	If ServiceProfileID is not provided these attributes are MANDATORY. If the-attributes are missing then the NAS SHALL silently discard this attribute and should reject the network entry of the MS.
307	ActivationTrigger	0-1	If ServiceProfileID is not provided these attributes are MANDATORY. If the-attributes are missing then the NAS SHALL silently discard this attribute and should reject the network entry of the MS.
308	TransportType	0-1	If ServiceProfileID is not provided these attributes are MANDATORY. If the-attributes are missing then the NAS SHALL silently discard this attribute and should reject the network entry of the MS.
309	UplinkQosID	0-1	This attribute SHALL be present if ServiceProfileId is not present and: Direction is Uplink or Direction is bi-directional and the flow is symmetrical.

TLV ID	TLV Name	Answer	Notes
			If ServiceProfileId or either of UplinkQoSID or DownlinkQoSID are missing then the NAS SHALL reject the network entry of the MS.
310	DownlinkQoSID	0-1	This attribute SHALL be present if ServiceProfileID is not present and: Direction is Downlink or Direction is bi-directional and not symmetrical. If ServiceProfileId or either of UplinkQoSID or DownlinkQoSID are missing then the NAS SHALL reject the network entry of the MS.
311	IP-Classifier	0-n	This attribute SHALL be present if ServiceProfileID is not present. If either are missing then the NAS SHALL reject the network entry of the MS.
349	Paging-Preference	0-1	This attribute is applicable to the downlink service flow only
350	VLANTagProcessingRuleID	0-1	This attribute MAY only be present for Ethernet service flows.

#### 1 5.5.2.64 VLANTagProcessing-Descriptor

<b>WType-ID</b>	211 for VLANTagProcessing-Descriptor
<b>Description</b>	This attribute describes the rules for the processing of the VLAN tags of an ETH packet flow. The VLANTagProcessing descriptor may be pre-provisioned.
<b>Value-Type</b>	Grouped

2

VLANTagProcessing-Descriptor ::= < AVP Header: 211 >

{ VLANTagProcessingRuleID }

{ C-VLAN-Priority-Setting }

[ VLAN-ID-Assignment ]

[ C-VLAN-ID ]

[ S-VLAN-ID ]

\* [ C-VID-To-S-VID-Mapping ]

[ Local-Config-Info ]

VLANTagProcessingRuleID = 0 is reserved with special meaning that no VLANTagProcessing is performed for the particular service flow regardless of any preprovisioned rule.

LocalConfigInfo is an arbitrary information element provided by the CSN in the case of preprovisioned R3 data path (Simple Ethernet), which

may be used for local configuration purposes. LocalConfigInfo is not used in the case of MIP based R3 data path.

\* [ AVP ]

1

### 2 5.5.2.65 WiMAX-Release

<b>WTYPE-ID</b>	301 for WiMAX-Release
<b>Description</b>	<p>In a Request specifies the WiMAX release of the sender. In an Answer specifies the release selected by the HAAA for this communication.</p> <p>AAA Proxies SHALL NOT alter the WiMAX-Release values received in an Answer command.</p> <p>If the NAS receives a WiMAX release that it does not support it SHALL treat the result as a rejection.</p> <p>If the HAAA receives a release that it does not support it SHALL respond back with an Answer with Result-Code set to DIAMETER_UNABLE_TO_COMPLY (5012) as defined by RFC3588.</p>
<b>Value Type</b>	UTF8String
<b>Value</b>	A string indicating a WiMAX release formatted as: major + "." + minor. For example, the first release of WiMAX is indicated as "1.0"

### 3 5.5.2.66 Accounting-Capabilities

<b>WType-ID</b>	302 for Accounting-Capabilities
<b>Description</b>	<p>In a Request describes the accounting capabilities that are supported by the sender (ASN or HA).</p> <p>In an Answer, describes the accounting capabilities that the server selected for the session.</p>
<b>Value-Type</b>	Unsigned32
<b>Value</b>	<p>In a request the NAS (ASN, HA) specifies the accounting capabilities that it supports as a bit-map. In an answer the server specifies one and only one of these options. All bits cleared 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 answer as a reject and it SHALL not provide any service to the MS. If there is a mismatch between Service Capability selection and Accounting Capability selection then the NAS SHALL treat the Answer as a rejection.</p> <ul style="list-style-type: none"> <li>• Bit #0 - IP/ETH-Session-based accounting. Default value for the ASN.</li> <li>• Bit #1 - Flow-based accounting.</li> <li>• Bit #2 - Flow-based accounting for ETH-CS.</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

#### 1 5.5.2.67 Hotlining-Capabilities

<b>WType-ID</b>	303 for Hotlining-Capabilities
<b>Description</b>	In a Request describes the Hot-Line capacities supported by the ASN or the HA.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	<p>In a request the NAS or HA specifies the Hot-Lining capabilities that it supports as a bit-map. All bits set to zero or the omission of this AVP means that Hot-Lining is not supported.</p> <ul style="list-style-type: none"> <li>• Bit #0 - Profile-based Hot-Lining is supported (using the Hotline-Profile-ID VSA)</li> <li>• Bit #1 - Rule-based Hot-Lining is supported using NAS-Filter-Rule</li> <li>• Bit #2 - Hot-Lining HTTP Redirection is supported.</li> <li>• Bit #3 - Rule-based Hot-Lining is supported using IP-Redirection rule.</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

#### 2 5.5.2.68 Idle-Mode-Notification-Capabilities

<b>WType-ID</b>	304 for Idle-Mode-Notification-Capabilities
<b>Description</b>	In a request or answer describes the idle mode notification capabilities supported by the ASN or required by the CSN. Omission of this AVP means that Idle Mode Notification is not supported or required.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	<p>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.</p> <ul style="list-style-type: none"> <li>• 0x0000 = Idle Mode notification is not supported or is not required.</li> <li>• 0x0001 = Idle Mode notification is supported or is required.</li> <li>• Rest of bits reserved</li> </ul>

#### 3 5.5.2.69 ServiceProfileID

<b>WType-ID</b>	305 ServiceProfileID
<b>Description</b>	This attribute identifies a pre-configure flow descriptor at the NAS.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer representing the identity of a Flow Spec that is pre-provisioned (most significant bit first). A value of zero(0) is invalid.

#### 4 5.5.2.70 Direction

<b>WType-ID</b>	306 for Direction
<b>Description</b>	The direction of the Packet Data Flow.
<b>Value-Type</b>	Enumerated
<b>Value</b>	<p>Octet enumeration with the following values:</p> <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = Uplink</li> <li>• 2 = Downlink</li> </ul>

	<ul style="list-style-type: none"> <li>• 3 = Bi-directional</li> <li>• 4 – FF = Reserved</li> </ul>
--	---

#### 1 5.5.2.71 Activation-Trigger

<b>WType-ID</b>	307 for Activation-Trigger
<b>Description</b>	<p>This parameter specifies the trigger to be used for the activation of the service flow. For the ISF, Provisioned, Admit and Activate SHALL be set.</p> <p>If “Dynamic-Reservation” is set to false, the QoS-Descriptor is used to specify a QoS profile for ISFs or pre-provisioned SFs.</p> <p>If “Dynamic-Reservation” is set to true, the QoS-Descriptor is used to specify a QoS profile for authorization checks done by the Anchor-SFA.</p>
<b>Value-Type</b>	Unsigned32
<b>Value</b>	<p>Octet bit-map with the following values:</p> <ul style="list-style-type: none"> <li>• Bit 0 = Reserved</li> <li>• Bit 1 = Provisioned (SHALL be set in case of ISF)</li> <li>• Bit 2 = Admit (SHALL be set in case of ISF)</li> <li>• Bit 3 = Activate (SHALL be set in case of ISF)</li> <li>• Bit 4 = Dynamic-Reservation(not valid for ISF)</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

#### 2 5.5.2.72 Transport-Type

<b>WType-ID</b>	308 for Transport-Type
<b>Description</b>	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].
<b>Value-Type</b>	Enumerated
<b>Value</b>	<p>Octet enumeration with the following values:</p> <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = IPv4-CS</li> <li>• 2 = IPv6-CS</li> <li>• 3 = Ethernet</li> <li>• 4 – 255 = Reserved</li> </ul>

#### 3 5.5.2.73 UplinkQoSID

<b>WType-ID</b>	309 for UplinkQoSID
<b>Description</b>	<p>The identifier of the QoS descriptor for the uplink direction or for bi-direction if the flow is bi-directional with symmetrical QoS.</p> <p>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.</p>
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.

#### 1 5.5.2.74 DownlinkQoSID

<b>WType-ID</b>	310 for DownlinkQoSID
<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.

#### 2 5.5.2.75 IP-Classifier

<b>WType-ID</b>	311 for IP-Classifier
<b>Description</b>	The classifier to match for traffic flowing in the uplink or 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.
<b>Value-Type</b>	Classifier as defined by ID- if Transport Type is 1 or 2 (IP-CS). Action is set to "permit". If the Transport Type is 3 (ETH-CS), it may contain the following EthFilterRule. The EthFilterRule should follow the format: action dir proto from src/mask to dst/mask [priority-range] [CVLAN-ID] action: <ul style="list-style-type: none"> <li>• "permit" - Allow packets that match the rule.</li> <li>• "deny" - Drop packets that match the rule.</li> </ul> dir: <ul style="list-style-type: none"> <li>• "in" is from the terminal</li> <li>• "out" is to the terminal.</li> </ul> proto: <ul style="list-style-type: none"> <li>• the ethernet type specified by number.</li> <li>• src and dst MAC address/mask</li> </ul> priority-range: <ul style="list-style-type: none"> <li>• specifies the priority range for the ethernet frame</li> </ul> CVLAN-ID: specifies the VLAN-ID range [VID-start, VID-end] for the ethernet frame.

#### 3 5.5.2.76 QoS-ID

<b>WType-ID</b>	312 for QoS-ID
<b>Description</b>	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)
<b>Value-Type</b>	Unsigned32
<b>Value</b>	An unsigned number less than 256.

#### 4 5.5.2.77 Global-Service-Class-Name

<b>WType-ID</b>	313 for Global-Service-Class-Name
-----------------	-----------------------------------

<b>Description</b>	This parameter represents the Global Service Class Name as defined in IEEE802.16e
<b>Value-Type</b>	OctetString
<b>Value</b>	String of length 6 octet containing the name of the global service class name. Values are defined in IEEE802.16e.

1 **5.5.2.78 Service-Class-Name**

<b>WType-ID</b>	314 for Service-Class-Name
<b>Description</b>	This parameter represents the Service Class Name as defined in IEEE802.16e
<b>Value-Type</b>	OctetString
<b>Value</b>	String containing the name of the service class name. Values are defined in IEEE802.16e.

2 **5.5.2.79 Schedule-Type**

<b>WType-ID</b>	315 for Schedule-Type
<b>Description</b>	The parameter specifies the Uplink Granted Scheduling Type as defined in IEEE802.16e.
<b>Value-Type</b>	Enumerated
<b>Value</b>	<p>The following values defined:</p> <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = Reserved</li> <li>• 2 = Best Effort</li> <li>• 3 = nrtPS</li> <li>• 4 = rtPS</li> <li>• 5 = Extended rtPS</li> <li>• 6 = UGS</li> <li>• 7 – 255 = Reserved</li> </ul> <p>Receivers MUST ignore reserved values.</p>

3 **5.5.2.80 Traffic-Priority**

<b>WType-ID</b>	316 for Traffic-Priority
<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	0 to 7 – Higher numbers indicate higher priority. Default 0.



1 **5.5.2.81 Maximum-Sustained-Traffic-Rate**

<b>WType-ID</b>	317 for Maximum-Sustained-Traffic-Rate
<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer specifying a rate in bits per second.

2 **5.5.2.82 Minimum-Reserved-Traffic-Rate**

<b>WType-ID</b>	318 for Minimum-Reserved-Traffic-Rate
<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer specifying the rate in bytes.

3 **5.5.2.83 Maximum-Traffic-Burst**

<b>WType-ID</b>	319 for Maximum-Traffic-Burst
<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer specifying the burst size in bytes per second as defined by IEEE802.16e.

4 **5.5.2.84 Tolerated-Jitter**

<b>WType-ID</b>	320 for Tolerated-Jitter
<b>Description</b>	Represents the Tolerated Jitter as defined in IEEE802.16e
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer representing the maximum delay variation (jitter) (in milliseconds).

5 **5.5.2.85 Maximum-Latency**

<b>WType-ID</b>	321 for Maximum-Latency
-----------------	-------------------------

<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned Integer specifying a maximum latency in units of milliseconds

1 **5.5.2.86 Reduced-Resources-Code**

<b>WType-ID</b>	322 for Reduced-Resources-Code
<b>Description</b>	This code indicates that the requesting entity will accept reduced resources if the requested resources are not available.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	A value of 0 is not allowed, value of 1 allowed. Other values are reserved.

2 **5.5.2.87 Media-Flow-Type**

<b>WType-ID</b>	323 for Media-Flow-Type
<b>Description</b>	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
<b>Value-Type</b>	Enumerated
<b>Value</b>	<p>An enumeration with the following values:</p> <ul style="list-style-type: none"> <li>• 0 = Reserved</li> <li>• 1 = Voice over IP</li> <li>• 2 = Robust Browser</li> <li>• 3 = Secure Browser/ VPN</li> <li>• 4 = Streaming video on demand</li> <li>• 5 = Streaming live TV</li> <li>• 6 = Music and Photo Download</li> <li>• 7 = Multi-player gaming</li> <li>• 8 = Location-based services</li> <li>• 9 = Text and Audio Books with Graphics</li> <li>• 10 = Video Conversation</li> <li>• 11 = Message</li> <li>• 12 = Control</li> <li>• 13 = Data</li> <li>• 14 – 255 = Reserved</li> </ul> <p>Receivers MUST ignore reserved values.</p>

3 **5.5.2.88 Unsolicited-Grant-Interval**

<b>WType-ID:</b>	325 for Unsolicited-Grant-Interval
<b>Description:</b>	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).
<b>Value-Type:</b>	Unsigned32
<b>Value:</b>	Value measuring time in milliseconds between 0 and $2^{16}-1$

#### 5.5.2.89 SDU-Size

<b>WType-ID</b>	326 for SDU-Size
<b>Description</b>	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.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Value $\leq 2^{16}-1$ . Default = 49

#### 5.5.2.90 Unsolicited-Polling-Interval

<b>WType-ID</b>	327 for Unsolicited-Polling-Interval
<b>Description</b>	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Unsigned integer representing the polling interval (in milliseconds) between 0 and $2^{16}-1$

#### 5.5.2.91 MN-HA-MIP4-MSA

<b>WType-ID</b>	328 for MN-HA-MIP4-MSA
<b>Description</b>	The MN-HA-MIP4-MSA VSA is a grouped AVP that describes the MN-HA security association used for MIP4 service.
<b>Value-Type</b>	Grouped

MN-HA-MIP4-MSA ::= < AVP Header: 328>

{ SA-SPI }

[ SA-Key ]

\*[AVP]

In a request this represents the SPI of the MN-HA MIP4 key being requested. In an answer, this is the SPI of the key being returned

The MN-HA MIP4 key.

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1

### 5.5.2.92 MN-vHA-MIP4-MSA

<b>WType-ID</b>	329 for MN-vHA-MIP4-MSA
<b>Description</b>	The MN-vHA-MIP4-MSA VSA is a grouped AVP that describes the MN-HA security association used for MIP4 service when the HA is allocated in the visited network.
<b>Value-Type</b>	Grouped

MN-vHA-MIP4-MSA ::= < AVP Header: 329>

{ SA-SPI }

In a request this represents the SPI of the MN-vHA MIP4 key being requested. In an answer, this is the SPI of the key being returned

[ SA-Key ]

The MN-HA MIP4 key.

\*[AVP]

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1

### 5.5.2.93 FA-RK-MSA

<b>WType-ID</b>	330 for FA-RK-MSA
<b>Description</b>	The FA-RK-MSA VSA is a grouped AVP that contains the security association of the root FA Key used to derive MN-FA security association
<b>Value-Type</b>	Grouped

FA-RK-MSA ::= < AVP Header: 330>

{ SA-SPI }

In a request this represents the SPI of the FA-Key key being requested. In an answer, this is the SPI of the key being returned

[ SA-Key ]

The Root key used to generate MN-FA keys.

\*[AVP]

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1

#### 5.5.2.94 HA-RK-MSA

<b>WType-ID</b>	331 for HA-RK-MSA
<b>Description</b>	The HA-RK-MSA VSA is a grouped AVP that contains the security association of the root HA Key used to derive FA-HA security association.
<b>Value-Type</b>	Grouped

HA-RK-MSA ::= < AVP Header: 331 >

{ SA-SPI }

In a request this represents the SPI of the key being requested. In an answer, this is the SPI of the key being returned

[ SA-Key ]

The key.

[ SA-Lifetime ]

The lifetime of the security association

\*[AVP]

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1
339	SA-Lifetime	0	1

#### 5.5.2.95 vHA-RK-MSA

<b>WType-ID</b>	332 for vHA-RK-MSA
<b>Description</b>	The vHA-RK-MSA VSA is a grouped AVP that contains the security association of the root HA Key used to derive FA-HA security association when the HA is allocated in the visited network.
<b>Value-Type</b>	Grouped

vHA-RK-MSA ::= < AVP Header: 332 >

{ SA-SPI }

In a request this represents the SPI of the key being requested. In an answer, this is the SPI of the key being returned

[ SA-Key ]

The key.

[ SA-Lifetime ]

The lifetime of the security association

\*[AVP]

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1
339	SA-Lifetime	0	1

#### 5.5.2.96 DHCP-RK-SA

<b>WType-ID</b>	333 for DHCP-RK-SA
<b>Description</b>	The DHCP-RK-SA VSA is a grouped AVP that contains the security parameters used to derive the security association between the DHCP relay and DHCP server.
<b>Value-Type</b>	Grouped

DHCP-RK-SA::= < AVP Header: 333>

{ SA-SPI }

In a request this represents the SPI of the key being requested. In an answer, this is the SPI of the key being returned

[ SA-Key ]

The key.

[ SA-Lifetime ]

The lifetime of the security association

\*[AVP]

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1
339	SA-Lifetime	0	1

#### 5.5.2.97 vDHCP-RK-SA

<b>WType-ID</b>	334 for vDHCP-RK-SA
<b>Description</b>	The vDHCP-RK-SA VSA is a grouped AVP that contains the security parameters used to derive the security association between the DHCP relay and DHCP server when the DHCP server is in the visited directory
<b>Value-Type</b>	Grouped

vDHCP-RK-SA::= < AVP Header: 334>

{ SA-SPI }

In a request this represents the SPI of the key being requested. In an answer, this is the SPI of the key being returned

[ SA-Key ]

The key.

[ SA-Lifetime ]

The lifetime of the security association

\*[AVP]

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1
339	SA-Lifetime	0	1

### 5.5.2.98 Redirect-Action

<b>WType-ID</b>	335 for Redirection-Action
<b>Description</b>	The action to perform when a classifier matches. PASS(0) means that if any of the classifiers matches take no redirection action. REDIRECT means that if any of the classifiers matches then redirect the packets. FLUSH means that all previous RULES MUST be deactivated.
<b>Value-Type</b>	Enumerated
<b>Value</b>	Valid enumeration values are: <ul style="list-style-type: none"> <li>PASS(0)</li> <li>REDIRECT(1)</li> <li>FLUSH(2)</li> </ul> All other values are reserved. Receivers MUST ignore reserved values.

### 5.5.2.99 Redirect-URL

<b>WType-ID</b>	336 for Redirected-URL
<b>Description</b>	A URL to be used as a redirection response.
<b>Value-Type</b>	UTF8String
<b>Value</b>	A URL as formatted by RFCXXX TBD

### 5.5.2.100 SA-SPI

<b>WType-ID</b>	337 for SA-SPI
<b>Description</b>	A Security Parameter Index.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Represents a Security Parameter Index.

### 5.5.2.101 SA-KEY

<b>WType-ID</b>	338 for SA-KEY
<b>Description</b>	A key.
<b>Value-Type</b>	OctetString

<b>Value</b>	The value of a KEY MSB first.
--------------	-------------------------------

#### 1 5.5.2.102 SA-Lifetime

<b>WType-ID</b>	339 for SA-Lifetime
<b>Description</b>	The lifetime in seconds of the security association
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Number of seconds.

#### 2 5.5.2.103 Redirect-Address

<b>WType-ID</b>	340 for Redirect-Address
<b>Description</b>	The IP address to redirect the traffic to.
<b>Value-Type</b>	Address
<b>Value</b>	The IPv4 address to redirect traffic to

#### 3 5.5.2.104 Redirect-Port

<b>WType-ID</b>	341 for Redirect-Port
<b>Description</b>	The redirection port to use as the destination port of a redirected packet.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	A port value in the range of 1 to 65356

#### 4 5.5.2.105 DHCPv6-RK-SA

<b>WType-ID</b>	342 for DHCPv6-RK-SA
<b>Description</b>	The DHCPv6-RK-SA VSA is a grouped AVP that contains the security parameters used to derive the security association between the DHCP relay and an IPv6 DHCP server.
<b>Value-Type</b>	Grouped

- 5 DHCPv6-RK-SA ::= < AVP Header: 342>
- |                 |  |
|-----------------|--|
| { SA-SPI }      | In a request this represents the SPI of the key being requested. In an answer, this is the SPI of the key being returned |
| [ SA-Key ]      | The key.   |
| [ SA-Lifetime ] | The lifetime of the security association   |
| *[AVP]          |  |

6

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1
339	SA-Lifetime	0	1



### 5.5.2.106 vDHCPv6-RK-SA

<b>WType-ID</b>	343 for vDHCPv6-RK-SA
<b>Description</b>	The vDHCPv6-RK-SA VSA is a grouped AVP that contains the security parameters used to derive the security association between the DHCP relay and an IPv6 DHCP server allocated in a visited network
<b>Value-Type</b>	Grouped

vDHCPv6-RK-SA ::= < AVP Header: 343>

{ SA-SPI }

In a request this represents the SPI of the key being requested. In an answer, this is the SPI of the key being returned

[ SA-Key ]

The key.

[ SA-Lifetime ]

The lifetime of the security association

\*[AVP]

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1
339	SA-Lifetime	0	1

### 5.5.2.107 Packet-Flow-Descriptor-Capabilities (This TLV is deprecated in this release)

<b>WType-ID</b>	344 for Packet-Flow-Descriptor-Capabilities (The usage of this TLV is deprecated in this release. Only Packet-Flow-Descriptor V2 SHALL be supported.)
<b>Description</b>	
<b>Value-Type</b>	
<b>Value</b>	•

### 5.5.2.108 Authorized-Network-Services

<b>WType-ID</b>	345 for Authorized-Network-Services
<b>Description</b>	This AVP is included in an Answer command to the NAS and indicates related Network Service Capabilities ASN is authorized to support.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Bit Mask with the following values: <ul style="list-style-type: none"> <li>• Bit #0 – CMIP4</li> <li>• Bit #1 – PMIP4</li> <li>• Bit #2 – Simple IPv4</li> </ul>

	<ul style="list-style-type: none"> <li>• Bit #3 – CMIP6</li> <li>• Bit #4 – Reserved</li> <li>• Bit #5 – Simple IPv6</li> <li>• Bit #6 – Simple ETH Service</li> <li>• Bit #7 – MIP based ETH Service</li> <li>• Bit #8 – L2 DHCP Relay<sup>[a]</sup></li> <li>• The rest of the bits are reserved. The sender SHALL set the reserved bits to zero, and the receiver SHALL ignore the values.</li> </ul>
--	--

#### 1 5.5.2.109 ASN-Network-Service-Capabilities

<b>WType-ID</b>	346 for ASN-Network-Service-Capabilities
<b>Description</b>	This AVP is included in a RADIUS Access-Request packet to the RADIUS server and indicates related Network Service Capabilities ASN is willing to support
<b>Value-Type</b>	Unsigned32
<b>Value</b>	<p>Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 – DHCPv4 Relay</li> <li>• Bit #1 – DHCPv6 Relay</li> <li>• Bit #2 – DHCPv4 Proxy</li> <li>• Bit #3 – DHCPv6 Proxy</li> <li>• Bit #4 – FA</li> <li>• Bit #5 – PMIP Client</li> <li>• Bit #6 – AR with IPv4 Transport<sup>36</sup></li> <li>• Bit #7 – AR with IPv6 Transport<sup>37</sup></li> <li>• Bit #8 – L2FW</li> <li>• Bit #9 – ETH Service FA</li> <li>• Bit #10 – L2 DHCP Relay</li> </ul> <p>All other bits are reserved. . The sender SHALL set the reserved bits to zero, and the receiver SHALL ignore the values.</p>

#### 2 5.5.2.110 VCSN-Network-Service-Capabilities

<b>WType-ID</b>	347 for VCSN-Network-Service-Capabilities
<b>Description</b>	This AVP is included in a Request packet to the Diameter server and indicates V-CSN related Network Service Capabilities
<b>Value-Type</b>	Unsigned32
<b>Value</b>	<p>Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 – DHCPv4 Server</li> <li>• Bit #1 – DHCPv6 Server</li> <li>• Bit #2 – HAv4</li> </ul>

<sup>36</sup> AR with IPv4 transport indicates the support of Simple IP service using IPv4 transport

<sup>37</sup> AR with IPv6 transport indicates the support of Simple IP service using IPv6 transport

	<ul style="list-style-type: none"> <li>• Bit #3 – HAv6</li> <li>• Bit #4 – eCB</li> <li>• Bit #5 – ETH HA</li> </ul> <p>All other bits are reserved. . The rest of the bits are reserved. The sender SHALL set the reserved bits to zero, and the receiver SHALL ignore the values.</p>
--	---

#### 1 5.5.2.111 Visited-Authorized-Network-Services

<b>WType-ID</b>	348 for Visited-Authorized-Network-Services
<b>Description</b>	This AVP is included in an Answer packet to the NAS and indicates whether V- and / or HCSN is authorized to anchor the ETH session or the IP session for Simple IP and PMIP services.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	<p>Bit Mask with the following values:</p> <ul style="list-style-type: none"> <li>• Bit #0 – CMIP4</li> <li>• Bit #1 – PMIP4</li> <li>• Bit #2 – Simple IPv4</li> <li>• Bit #3 – CMIP6</li> <li>• Bit #4 – PMIP6</li> <li>• Bit #5 – Simple IPv6</li> <li>• Bit #6 – Simple ETH Service</li> <li>• Bit#7 – MIP based ETH Service</li> <li>• Bit#8 – L2 DHCP Relay<sup>[a]</sup></li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

#### 2 5.5.2.112 Paging-Preference

<b>WType-ID</b>	349 for Paging-Preference
<b>Description</b>	This parameter is a single bit indicator of an MS's preference for the reception of paging advisory messages during idle mode. When set, it indicates that the BS may present paging advisory messages or other indicative messages to the MS when data SDUs bound for the MS are present while the MS is in idle mode.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Refer to 802.16e section 11.13.30.

#### 3 5.5.2.113 VLANTagProcessingRuleID

<b>WType-ID</b>	350 for VLANTagProcessingRuleID
<b>Description</b>	The ID of the rules for assigning priority bits and VLAN-IDs in Ethernet frames
<b>Value-Type</b>	Unsigned32
<b>Value</b>	Containing the VLAN Tag Processing Rule ID of the rules for processing the VLAN tags in Ethernet frames

#### 4 5.5.2.114 Media-Flow-Description-In-SDP-Format

<b>WType-ID</b>	351 for Media-Flow-Description-In-SDP-Format
-----------------	--

<b>Description</b>	This is a variable length string having SDP information. The <SDP string> is encoded as specified in IETF RFC 2327
<b>Value-Type</b>	UTF8String
<b>Value</b>	<SDP string> is encoded as specified in IETF RFC 2327.

#### 1 5.5.2.115 Transmission-Policy

<b>WType-ID</b>	352 for Transmission-Policy
<b>Description</b>	The parameter indicates the transmission policy of a service flow.
<b>Value-Type</b>	Unsigned32
<b>Value</b>	<p>Octet enumeration with the following values defined:</p> <ul style="list-style-type: none"> <li>• Bit #0 – Service flow SHALL NOT use broadcast bandwidth request opportunities. (Uplink only)</li> <li>• Bit #1 –Service flow SHALL NOT use multicast bandwidth request opportunities. (Uplink only).</li> <li>• Bit #2 – The service flow SHALL NOT piggyback requests with data. (Uplink only)</li> <li>• Bit #3 – The service flow SHALL NOT fragment data.</li> <li>• Bit #4 – The service flow SHALL NOT suppress payload headers (CS parameter).</li> <li>• Bit #5 – The service flow SHALL NOT pack multiple SDUs (or fragments) into single MAC PDUs.</li> <li>• Bit #6 – The service flow SHALL NOT include CRC in the MAC PDU.</li> <li>• Bit #7 – The service flow SHALL NOT compress payload headers using ROHC.</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p> <p>Note: The bit#7 is reserved prior to NWG release 1.5</p>

#### 2 5.5.2.116 Classifier

<b>WType-ID</b>	353 for Classifier
<b>Description</b>	<p>The classifier to match for traffic flowing in the direction indicated by the direction encoded in the classifier.</p> <p>Classifiers for the appropriate direction are evaluated in order, with the first matched rule terminating the evaluation.</p> <p>If the classifier cannot be parsed then the NAS SHALL reject the network entry of the MS.</p>
<b>Value-Type</b>	Grouped as per draft-ietf-dime-qos-attributes-11.txt [85] with a few modifications as noted below.

3

Classifier::= < AVP Header: 353>

{ ClassifierID }	Unique within the parent container.
{ Priority }	Unique within the parent container.
{ Direction }	
{ Action }	
[ Protocol ]	
[ From-Spec ]	

[ To-Spec ]

[ IP-TOS/DSCP-Range-And-Mask ]

[ ETH-Option ]

May only present in case of Ethernet based transport.

\*[AVP]

AVP	TLV Name	Request	Answer
354	Classifier-ID	0	1
355	Priority	0	1
306	Direction	0	1
357	Action	0	1
358	Protocol	0	0-1
359	From-Specification	0	0-1
360	To-Specification	0	0-1
361	IP-TOS/DSCP-Range-And-Mask	0	0-1
362	ETH-Option	0	0-1

#### 5.5.2.117 Classifier-ID

<b>WType-ID</b>	354 for Classifier-ID
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]. An identifier of the classifier that uniquely identifies the classifier in the scope of the Packet-Flow-Descriptor irrespective of whether or not the classifier is an uplink or downlink classifier.
<b>Value-Type</b>	OctetString as per draft-ietf-dime-qos-attributes-11.txt [85]. In WiMAX the identifier is unique within the scope of the parent container.

#### 5.5.2.118 Priority

<b>WType-ID</b>	355 for Priority
<b>Description</b>	The value of the field specifies the priority for processing this classifier relative to other classifiers. It is expected to be unique across all packet data flows for a given direction (uplink/downlink). A bidirectional packet data flow can be considered as both uplink and downlink.
<b>Value-Type</b>	Unsigned32. Value range is between 0 and 255. The higher the value the higher the priority

#### 5.5.2.119 Direction

<b>WType-ID</b>	356 for Direction
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]. The Direction AVP specifies in which direction to apply the Classifier. The values of the enumeration are: "IN","OUT","BOTH".



[ IP-Address-Range ]

source specification. If the IP address TLVs are missing then comparison of the IP address field is irrelevant.

Only one IPAddress, IPAddressRange, or IPAddressMask may appear in a source specification. If the IP address TLVs are missing then comparison of the IP address field is irrelevant.

This attribute is used only by the network for downlink traffic. It is not sent to the MS.

[ IP-Address-Mask ]

Only one IPAddress, IPAddressRange, or IPAddressMask may appear in a source specification. If the IP address TLVs are missing then comparison of the IP address field is irrelevant.

[ Port ]

If one of the Port(s) matches, there is no need to check the PortRange; or if one of the PortRange(s) matches then there is no need to check the Ports. The order of checking SHALL be in the order that they appear in the container. If the port TLVs are missing then comparison of the port field is irrelevant.

This attribute is used only by the network for downlink traffic. It is not sent to the MS.

[ Port-Range ]

If one of the Port(s) matches, there is no need to check the PortRange; or if one of the PortRange(s) matches, then there is no need to check the Ports. The order of checking SHALL be in the order that they appear in the container. If the port TLVs are missing then comparison of the port field is irrelevant.

[ Negated ]

Inverts the notion of the IP address fields (1,2,3 and 7). It does not impact the port or port range specification. Inverted MAY only appear when one or more of the IP Address fields (1,2,3 and 7) appear. Otherwise the source/destination specification is in error.

This attribute is used only by the network for downlink traffic. It is not sent to the MS.

[User-Assigned-Address ]

This attribute is used only by the network for downlink traffic. It is not sent to the MS.

[ MAC-Address ]

Only valid for ETH-CS.

[ MAC-Mask ]

Only valid for ETH-CS.

\*[AVP]

AVP	TLV Name	Request	Answer
374	IP-Address	0	0-1
375	IP-Address-Range	0	0-1
376	IP-Address-Mask	0	0-1
377	Port	0	0-n
378	Port-Range	0	0-n
379	Negated	0	0-1
380	User-Assigned-Address	0	0-1
381	MAC-Address	0	0-1
382	MAC-Mask	0	0-1

### 5.5.2.123 To-Spec

<b>WType-ID</b>	360 for To-Specification
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85] Contains a destination specification for a packet. When the direction attribute is set to bi-direction the Destination Specification(s) is compared to the Destination field of the IN coming packets and the Source field of the OUT going packets. If this field is omitted, then comparison of the destination IP and port or destination MAC address for this entry is irrelevant.
<b>Value-Type</b>	Grouped as per draft-ietf-dime-qos-attributes-11.txt [85]

To-Spec::= < AVP Header: 360>

[ IP-Address ]

Only one IPAddress, IPAddressRange, or IPAddressMask may appear in a source specification. If the IP address TLVs are missing then comparison of the IP address field is irrelevant.

[ IP-Address-Range ]

Only one IPAddress, IPAddressRange, or IPAddressMask may appear in a source specification. If the IP address TLVs are missing then comparison of the IP address field is irrelevant.

This attribute is used only by the network for downlink traffic. It is not sent to the MS.

[ IP-Address-Mask ]

Only one IPAddress, IPAddressRange,



[ Port ]

or IPAddressMask may appear in a source specification. If the IP address TLVs are missing then comparison of the IP address field is irrelevant.

If one of the Port(s) matches, there is no need to check the PortRange; or if one of the PortRange(s) matches, then there is no need to check the Ports. The order of checking SHALL be in the order that they appear in the container. If the port TLVs are missing then comparison of the port field is irrelevant.

This attribute is used only by the network for downlink traffic. It is not sent to the MS.

[ Port-Range ]

If one of the Port(s) matches, there is no need to check the PortRange; or if one of the PortRange(s) matches, then there is no need to check the Ports. The order of checking SHALL be in the order that they appear in the container. If the port TLVs are missing then comparison of the port field is irrelevant.

[ Negated ]

Inverts the notion of the IP address fields (1,2,3 and 7). It does not impact the port or port range specification. Inverted MAY only appear when one or more of the IP Address fields (1,2,3 and 7) appear. Otherwise the source/destination specification is in error.

This attribute is used only by the network for downlink traffic. It is not sent to the MS.

[User-Assigned-Address ]

This attribute is used only by the network for downlink traffic. It is not sent to the MS.

[ MAC-Address ]

Only valid for ETH-CS.

[ MAC-Mask ]

Only valid for ETH-CS.

\*[AVP]

1

AVP	TLV Name	Request	Answer
374	IP-Address	0	0-1
375	IP-Address-Range	0	0-1

376	IP-Address-Mask	0	0-1
377	Port	0	0-n
378	Port-Range	0	0-n
379	Negated	0	0-1
380	User-Assigned-Address	0	0-1
381	MAC-Address	0	0-1
382	MAC-Mask	0	0-1

#### 5.5.2.124 IP-TOS/DSCP-Range-And-Mask

<b>WType-ID</b>	361 for IP-TOS/DSCP-Range-And-Mask
<b>Description</b>	The values of the field specify the matching parameters for the IP type of service/DSCP [29] 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.
<b>Value-Type</b>	Unsigned32. The first (least significant) octet represents the lower limit of the ToS, the second octet represent the higher limit of the ToS and the last octet represents the mask value. The most significant octet is reserved. The sender must set the value to zero and the receiver SHALL ignore the value.

#### 5.5.2.125 ETH-Option

<b>WType-ID</b>	362 for ETH-Option
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]. A grouped TLV with Ethernet specific attributes.
<b>Value-Type</b>	Grouped

ETH-Option ::= < AVP Header: 362 >

{ ETH-Proto-Type }

[ VLAN-ID-Range ]

\*[ ETH-Priority-Range ]

\* [ AVP ]

In WiMAX this attribute may only appear once.

#### 5.5.2.126 ETH-Proto-Type

<b>WType-ID</b>	363 for ETH-Proto-Type
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]. Specifies Ethertype and DSAP
<b>Value-Type</b>	Grouped

ETH-Proto-Type ::= < AVP Header: 363 >

\*[ ETH-Ether-Type ]

Both attributes MAY be absent but only one of ETH-Ether-Type or ETH-Sap SHALL be present.

\*[ ETH-Sap ]

\* [ AVP ]

### 5.5.2.127 VLAN-ID-Range

<b>WType-ID</b>	364 for VLAN-ID-Range
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]. If present, this field specifies the matching values for the VLAN-ID bits. If omitted, the VLAN-ID bits are irrelevant for this entry.
<b>Value-Type</b>	Grouped

VLAN-ID-Range::= < AVP Header: 364>

[ S-VID-Start ]

[ S-VID-End

[ C-VID-Start ]

[ C-VID-End ]

\* [ AVP ]

### 5.5.2.128 ETH-Priority-Range

<b>WType-ID</b>	365 for ETH-Priority-Range
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Grouped

ETH-Priority-Range::= < AVP Header: 365>

[ ETH-Low-Priority]

[ ETH-High-Priority]

\* [ AVP ]

### 5.5.2.129 ETH-Ether-Type

<b>WType-ID</b>	366 for ETH-Ether-Type
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	OctetString. The value is a double octet that contains the value of the Ethertype field in the packet to match. This AVP MAY be present in the case of DIX or if SNAP is present at 802.2 but the ETH-SAP AVP MUST NOT be present in this case.

1 **5.5.2.130 ETH-SAP**

<b>WType-ID</b>	367 for ETH-SAP
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	OctetString. The value is a double octet representing the 802.2 SAP as specified in [IEEE802.2]. The first octet contains the DSAP and the second the SSAP.

2 **5.5.2.131 S-VID-Start**

<b>WType-ID</b>	368 for S-VID-Start
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Unsigned32 with values between 0 and 4095 inclusive.

3 **5.5.2.132 S-VID-End**

<b>WType-ID</b>	369 for S-VID-End
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Unsigned32 with values between 0 and 4095 inclusive.

4 **5.5.2.133 C-VID-Start**

<b>WType-ID</b>	370 for C-VID-Start
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Unsigned32 with values between 0 and 4095 inclusive.

5 **5.5.2.134 C-VID-End**

<b>WType-ID</b>	371 for C-VID-End
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Unsigned32 with values between 0 and 4095 inclusive.

6 **5.5.2.135 ETH-Low-Priority**

<b>WType-ID</b>	372 for ETH-Low-Priority
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Unsigned32 with values between 0 and 7 inclusive.

7 **5.5.2.136 ETH-High-Priority**

<b>WType-ID</b>	373 for ETH-High-Priority
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Unsigned32 with value between 0 and 7 inclusive.

8 **5.5.2.137 IP-Address**

<b>WType-ID</b>	374 for IP-Address
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]

<b>Value-Type</b>	Address. IPv4 or IPv6 Address.
-------------------	--------------------------------

#### 5.5.2.138IP-Address-Range

<b>WType-ID</b>	375 for IP-Address-Range
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Grouped

IPAddressRange::= < AVP Header: 375>

[ IP-Address-Start ]

[ IP-Address-End ]

\* [ AVP ]

#### 5.5.2.139IP-Address-Mask

<b>WType-ID</b>	376 for IP-Address-Mask
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Grouped.

IP-Address-Mask::= < AVP Header: 376>

[ IP-Address ]

[ IP-Bit-Mask-Width ]

\* [ AVP ]

#### 5.5.2.140Port

<b>WType-ID</b>	377 for Port
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Integer32 with a value of 0 to 65535.

#### 5.5.2.141Port-Range

<b>WType-ID</b>	378 for Port-Range
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Grouped

Port-Range::= < AVP Header: 378>

[ Port-Start ]

[ Port-End ]

\* [ AVP ]

#### 5.5.2.142 Negated

<b>WType-ID</b>	379 for Negated
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Enumerated containing the following values: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul> All other values reserved

#### 5.5.2.143 User-Assigned-Address

<b>WType-ID</b>	380 for User-Assigned-Address
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Enumerated with values: <ul style="list-style-type: none"> <li>• TRUE</li> <li>• FALSE</li> </ul> All other values reserved.

#### 5.5.2.144 MAC-Address

<b>WType-ID</b>	381 for MAC-Address
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85].
<b>Value-Type</b>	OctetString the value is a 6 octet encoding of the MAC Address as it would appear in the frame header.

#### 5.5.2.145 MAC-Mask

<b>WType-ID</b>	382 for MAC-Mask
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Grouped

MAC-Mask ::= < AVP Header: 382>

[ MAC-Address ]

[ MAC-Address-Mask-Pattern ]

\* [ AVP ]

#### 5.5.2.146 IP-Address-Start

<b>WType-ID</b>	383 for IP-Address-Start
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Address. Representing IPv4 or IPv6 address.

1 **5.5.2.147 IP-Address-End**

<b>WType-ID</b>	384 for IP-Address-End
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Address. Representing IPv4 or IPv6 address.

2 **5.5.2.148 IP-Bit-Mask-Width**

<b>WType-ID</b>	385 for IP-Bit-Mask-Width
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Unsigned32 specifying a number of bits.

3 **5.5.2.149 Port-Start**

<b>WType-ID</b>	386 for Port-Start
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Integer32 with value from 0 to 65535 inclusive representing a port number

4 **5.5.2.150 Port-End**

<b>WType-ID</b>	387 for Port-End
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	Integer32 with value from 0 to 65535 inclusive, representing a port number.

5 **5.5.2.151 MAC-Address-Mask-Pattern**

<b>WType-ID</b>	388 for MAC-Address-Mask-Pattern
<b>Description</b>	As per draft-ietf-dime-qos-attributes-11.txt [85]
<b>Value-Type</b>	OctetString. The value is 6 octets specifying the bit positions of a MAC address that are taken for matching.

6 **5.5.2.152 C-VLAN-Priority-Setting**

<b>WType-ID</b>	389 for C-VLAN-Priority-Setting
<b>Description</b>	Defines the setting of the priority_bits in the C-VLAN tag in the upstream direction.
<b>Value-Type</b>	Unsigned32 representing a bit-field as follows: <ul style="list-style-type: none"> <li>0x00000000 = forward the p_bits without modification</li> <li>0x0000001x = drop frames with p_bits set to a higher value than x</li> <li>0x0000002x = set p_bits to x when p_bits set to a higher value than x</li> <li>0x0000003x = set the p_bits to x: insert VLAN tag with VLAN-ID=0 and p_bits set to value x into Ethernet frames without VLAN tag.</li> </ul> Other values reserved

7 **5.5.2.153 VLAN-ID-Assignment**

<b>WType-ID</b>	390 for VLAN-ID-Assignment
<b>Description</b>	Defines the processing of the C-VLAN tag and S-VLAN tag

<b>Value-Type</b>	<p>Unsigned32 value representing a bit-field as follows:</p> <ul style="list-style-type: none"> <li>• 0x00000000 = forward VLAN tags without modification</li> <li>• 0x00000010 = remove S-VID in downstream direction</li> <li>• 0x00000020 = remove C-VID and S-VID, if present, in downstream direction</li> <li>• 0x0000010x = add C-VLAN tag in upstream to frames without C-VLAN tag with C-VID set to C-VLAN ID and p_bits set to x</li> <li>• 0x0000020x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set to S-VLAN ID and S-p_bits set to x</li> <li>• 0x00000280 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set to S-VLAN ID and S-p_bits copied from C-p_bits</li> <li>• 0x0000040x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C-&gt;S-VID Mapping table and S-p_bits set to x If no entry exists for a particular C-VID in the C-&gt;S-VID Mapping table, the S-VID is set to 0</li> <li>• 0x00000480 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C-&gt;S-VID Mapping Table and S-p_bits copied from C-p_bits If no entry exists for a particular C-VID in the C-&gt;S-VID Mapping table, the S-VID is set to 0</li> </ul> <p>Other values reserved.</p> <p>Note: One downstream rule can be combined (ORed) with one upstream rule.</p>
-------------------	---

1 **5.5.2.154 C-VLAN-ID**

<b>WType-ID</b>	391 for C-VLAN-ID
<b>Description</b>	The value of the field specifies the CVALN ID value for the Ethernet frame.
<b>Value-Type</b>	Unsigned32

2 **5.5.2.155 S-VLAN-ID**

<b>WType-ID</b>	392 for MAC-Address-Mask-Pattern
<b>Description</b>	The value of the field specifies the SVALN ID value for the Ethernet frame.
<b>Value-Type</b>	Unsigned32

3 **5.5.2.156 C-VID-To-S-VID-Mapping**

<b>WType-ID</b>	393 for C-VID-To-S-VID-Mapping
<b>Description</b>	The value of the field specifies a mapping between a C-VID and a S-VID
<b>Value-Type</b>	Unsigned32. C-VID,S-VID

4 **5.5.2.157 Local-Config-Info**

<b>WType-ID</b>	394 for Local-Config-Info
<b>Description</b>	Local configuration information for preprovisioned R3 data path (Simple Ethernet)
<b>Value-Type</b>	<p>OctetString of length n containing arbitrary information</p> <p>The meaning of the information in LocalConfigInfo is subject of static configuration agreements between NAP and NSP.</p>



### 5.5.2.158hDHCP-Server-Parameters

<b>WType-ID</b>	86 for hDHCP-Server-Parameters
<b>Description</b>	This attribute contains the Home DHCP server and corresponding security keys.
<b>Value-Type</b>	Grouped

IP-Address-Mask::= < AVP Header: 86>

[hDHCPv4-Server]  
[hDHCPv6-Server]  
[DHCP-RK]  
[DHCP-RK-Key-ID]  
[DHCP-RK-Lifetime]  
\* [ AVP ]

AVP	TLV Name	Request	Answer
8	hDHCPv4-Server	0	0-1
9	hDHCPv6-Server	0	0-1
40	DHCP-RK	0	0-1
41	DHCP-RK-Key-ID	0	0-1
42	DHCP-RK-Lifetime	0	0-1

### 5.5.2.159vDHCP-Server-Parameters

<b>WType-ID</b>	87 for vDHCP-Server-Parameters
<b>Description</b>	This attribute contains a Visited DHCPv4 server and corresponding security keys.
<b>Value-Type</b>	Grouped

IP-Address-Mask::= < AVP Header: 87>

[vDHCPv4-Server]  
[vDHCPv6-Server]  
[DHCP-RK]  
[DHCP-RK-Key-ID]  
[DHCP-RK-Lifetime]  
\* [ AVP ]

AVP	TLV Name	Request	Answer
73	vDHCPv4-Server	0-1	0-1

74	vDHCPv6-Server	0-1	0-1
40	DHCP-RK	0	0-1
41	DHCP-RK-Key-ID	0	0-1
42	DHCP-RK-Lifetime	0	0-1

### 5.5.2.160 DSCP

<b>WType-ID</b>	458 for DSCP
<b>Description</b>	<u>Differentiated services code point as defined in RFC 2474. Used to mark the IP packets of the flow. See RFC3246, RFC2597 and RFC4595 for recommended values.</u>
<b>Value-Type</b>	<u>Unsigned One Octet representing the DSCP field as defined in RFC2474.</u>

### 5.5.2.161 BS-Location

<b>WType-ID</b>	88 for BS-Location
<b>Description</b>	In an WDER Command the VSA may be used as an alternative Serving BS identifier and usually indicates the location information of the BS which may be described as Lat/Long/Sector/Carrier information of the serving BS.
<b>Value-Type</b>	UTF8String representing location.

### 5.5.2.162 Mobility-Access-Classifer

<b>WType-ID</b>	89 for Mobility-Access-Classifer
<b>Description</b>	In a WDEA Command the VSA identifies the classification of the subscriber at the H-AAA as a fixed, nomadic or mobile access subscriber.
<b>Value-Type</b>	Unsigned32 representing an enumeration with the following values: <ul style="list-style-type: none"> <li>• 1 = Fixed</li> <li>• 2 = Nomadic</li> <li>• 3 = Mobile</li> </ul> 4-255= Reserved Receivers MUST ignore reserved values

### 5.5.2.163 Mobility-Access-Capabilities

<b>WType-ID</b>	395 for Mobility-Access-Capabilities
<b>Description</b>	In a request describes the mobility access capabilities supported by the ASN. Omission of this AVP means fixed/nomadic access is not supported.
<b>Value-Type</b>	Unsigned32. In a Request the NAS (ASN) specifies if fixed/nomadic access is supported at the ASN. <ul style="list-style-type: none"> <li>• Bit#0 = Fixed/Nomadic access is not supported. Only Mobility.</li> <li>• Bit#1 = Fixed/Nomadic access is supported alongside Mobility.</li> <li>• Bit#2 = Only Fixed/Nomadic access is supported. No Mobility</li> </ul> All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

### 1 5.5.2.164 ROHC-Support

<b>WType-ID</b>	396 for ROHC-Support
<b>Description</b>	In an Access-Request or Accept-Accept describes the ROHC capability supported by the ASN or required by the CSN. Omission of this sub TLV means that ROHC capability is not supported or required.
<b>Value-Type</b>	<p>Unsigned32.</p> <p>In a request the NAS (ASN) specifies if ROHC capability is supported at the ASN. In an answer the HAAA specifies if ROHC capability is required. A value of zero or the omission of this subTLV means that ROHC is not supported.</p> <ul style="list-style-type: none"> <li>• Bit #0 = ROHC capability is supported or is required.</li> </ul> <p>All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits..</p>

### 2 5.5.2.165 R3-OC-Session-Continue

<b>WType-ID</b>	416 for R3-OC-Session-Continue
<b>Description</b>	<p>If the R3-OC-Session-Continue AVP has been provided in initial CCR message, its presence indicates that this CCR message is triggered as a result of a PPC relocation.</p> <p>If the R3-OC-Session-Continue AVP has been provided in CCA message, its presence indicates that this CCA message is the response to the CCR with R3-OC-Session-Continue AVP present. If absent, the client SHALL assume the value “FALSE”.</p>
<b>Value-Type</b>	<p>Enumerated.</p> <p>The following values are defined:</p> <p>FALSE (0)</p> <p>The R3-OC-Session-Continue AVP with value of FALSE (0) SHALL NOT be present in the CCR message. Its presence in CCA indicates a new session SHALL be created, and the old session terminated.</p> <p>TRUE (1)</p> <p>Its presence in CCR message indicates this CCR message is triggered by the PPC relocation. Its presence in the CCA message indicates the old session SHALL be continued, and no new session to be created.</p>

### 3 5.5.2.166 Old-Session-Id

<b>WType-ID</b>	406 for Old-Session-Id
<b>Description</b>	<p>The old-Session-Id holds the session-id of the session between the old A-PCEF/PPC and the OCS/PPS. It is included in the first CCR message from the new A-PCEF/PPC to the OCS/PPS to enable the OCS/PPS to correlate the new Diameter session with an existing UE session.</p> <p>(The new A-PCEF/PPC obtains the Old Session-Id during the A-PCEF/PPC relocation procedure described in section 4.4.3.3.6.)</p>
<b>Value-Type</b>	UTF8String

### 4 5.5.2.167 WiMAX-Information

<b>WType-ID</b>	409 for WiMAX-Information
-----------------	---------------------------

<b>Description</b>	The <i>WiMAX-Information</i> AVP contains WiMAX access network accounting information for the offline and online charging.
<b>Value-Type</b>	Grouped

1

<WiMAX-Information> ::= < AVP Header: 409 >

- [ Acct-Session-Id ]
- [ Acct-Multi-Session-Id ]
- [ Acct-Delay-Time ]
- [ NAS-Identifier ]
- [ NAS-Port-Type ]
- [ Class ]
- [ Termination-Cause ]
- [ Accounting-Input-Octets ]
- [ Accounting-Input-Packets ]
- [ Accounting-Output-Octets ]
- [ Accounting-Output-Packets ]
- [ Acct-Link-Count ]
- [ Acct-Session-Time ]
- [ Calling-Station-Id ]
- [ Framed-IP-Address ]
- [ Framed-IPv6-Prefix ]
- [ Framed-Interface-Id ]
- [ CUI ]
- [ Session-Continue ]
- [ Beginning-Of-Session ]
- [ IP-Technology ]
- [ Hotline-Indication ]
- [ Hotlining-Capabilities ]
- [ Prepaid-Indicator ]
- [ Idle-Mode-Transition ]
- [ Count-Type ]
- [ hHA-IP-MIP4 ]
- [ hHA-IP-MIP6 ]
- [ NAP-ID ]
- [ NSP-ID ]
- [ BS-ID ]
- [ Location ]

[ GMT-Time-Zone-Offset ]  
 [ Active-Time ]  
 [ Control-Packets-In ]  
 [ Control-Packets-Out ]  
 [ Control-Octets-In ]  
 [ Control-Octets-Out ]  
 \* [ Uplink-Flow-Description ]  
 \* [ Downlink-Flow-Description ]  
 [ Uplink-Granted-QoS ]  
 [ Downlink-Granted-QoS ]  
 [ Visited-Framed-IP-Address ]  
 [ Visited-Framed-IPv6-Prefix ]  
 [ Visited-Framed-Interface-Id ]  
 [ Direction ]  
 [ Interim-Cause ]  
~~[ WiMAX-QoS-Information ]~~  
~~[ AF-Correlation-Information ]~~  
~~[ AF-Charging-Identifier ]~~  
 [ Access-Network-Charging-Identifier-Gx ]  
 [ Access-Network-Charging-Address ]  
 [ R3-OC-Session-Continue ]  
 [ Old-Session-Id ]  
 [ Offline-Charging ]

Only used in case of PCC. See [3] for further details.

Only used in case of PCC. See [3] for further details.

Only used in case of PCC. See [3] for further details.

### 5.5.2.168 Uplink-Granted-QoS

<b>WType-ID</b>	30 for Uplink-Granted-QoS
<b>Description</b>	The Uplink-Granted-QoS AVP specifies the Uplink QoS granted to the MS
<b>Value-Type</b>	Grouped

Uplink-Granted-QoS ::= < AVP Header: 30 >

[ QoS-ID ]  
 [ Global-Service-Class-Name ]  
 [ Service-Class-Name ]  
 [ Schedule-Type ]

[ Traffic-Priority ]  
 [ Maximum-Sustained-Traffic-Rate ]  
 [ Minimum-Reserved-Traffic-Rate ]  
 [ Maximum-Traffic-Burst ]  
 [ Tolerated-Jitter ]  
 [ Maximum-Latency ]  
 [ Reduced-Resources-Code ]  
 [ Media-Flow-Type ]  
 [ Unsolicited-Polling-Interval ]  
 [ Media-Flow-Description-In-SDP-Format ]  
 [ Transmission-Policy ]  
 [ Unsolicited-Grant-Interval ]  
 [ SDU-Size ]

1

## 2 5.5.2.169 Downlink-Granted-QoS

<b>WType-ID</b>	63 for Downlink-Granted-QoS
<b>Description</b>	The <i>Downlink-Granted-QoS</i> AVP specifies Downlink QoS granted to the MS.
<b>Value-Type</b>	Grouped

3

Downlink-Granted-QoS :: = < AVP Header: 63 >

[ QoS-ID ]  
 [ Global-Service-Class-Name ]  
 [ Service-Class-Name ]  
 [ Schedule-Type ]  
 [ Traffic-Priority ]  
 [ Maximum-Sustained-Traffic-Rate ]  
 [ Minimum-Reserved-Traffic-Rate ]  
 [ Maximum-Traffic-Burst ]  
 [ Tolerated-Jitter ]  
 [ Maximum-Latency ]  
 [ Reduced-Resources-Code ]  
 [ Media-Flow-Type ]  
 [ Unsolicited-Polling-Interval ]  
 [ Media-Flow-Description-In-SDP-Format ]  
 [ Transmission-Policy ]  
 [ Unsolicited-Grant-Interval ]

[ SDU-Size ]

1

### 2 5.5.2.170 Interim-Cause

<b>WType-ID</b>	413 for Interim-Cause
<b>Description</b>	The <i>Interim-Cause</i> AVP is used to indicate the reason why the accounting interim message was generated by the accounting client.
<b>Value-Type</b>	Enumerated. The following values are defined:  INTERIM_INTERVAL (1) Interim message was generated by the accounting interim interval timer. IDLE_MODE_TRANSITION (2) Interim message was generated upon the idle mode transition.

### 3 5.5.2.171 MS-Authenticated

<b>WType-ID</b>	90 for MS-Authenticated
<b>Description</b>	A flag indicating whether the MS has successfully performed device authentication during initial network entry or not.
<b>Value-Type</b>	Enumerated. Allowed values:  (0) The MS has not performed device authentication. (1) The MS has successfully performed device authentication during initial network entry as part of which the MAC address has also been authenticated.  All other values reserved

### 4 5.5.2.172 Release-Supported

<b>WType-ID</b>	397 for Release-Supported
<b>Description</b>	This TLV is included in a AAA request message to the HAAA and indicates which WiMAX versions are supported by the NAS or by the VAAA (if the VAAA is participating in the version negotiation). The attribute SHALL NOT be sent in a AAA Answer message.
<b>Value-Type</b>	OctetString. String of supported releases separated by commas ','. The list is ordered from the lowest version to the highest version supported

### 5 5.5.2.173 Version-Negotiation-Flag

<b>WType-ID</b>	398 for Version-Negotiation-Flag
<b>Description</b>	This TLV SHALL be included in a AAA request message by the VAAA to indicate that the VAAA is agreeing with the proposed version by the NAS or if it is proposing its own version in the WiMAX-Release TLV.  The attribute MAY be included in the AAA answer message set to the value of three(3) by the HAAA to indicate to the VAAA and NAS that the Challenge message is announcing the negotiated version only. The NAS will have to re-issue the request message encode with the version proposed in the WiMAX Release TLV of the WiMAX-Capability

	attribute.
<b>Value-Type</b>	Enumerated. Allowed values: <ul style="list-style-type: none"> <li>(1) Indicating that the VAAA has agreed to the version proposed by the NAS. This implies that the Diameter WDER is coded in accordance with the indicated WiMAX-Release.</li> <li>(2) Indicates that the VAAA has modified the version proposed by the NAS. This means that the HAAA SHALL use this exchange for version negotiation only.</li> <li>(3) Set by the HAAA to indicate that the Diameter WDEA(Multi-round) is for version negotiation only.</li> </ul> All other values are reserved.

#### 5.5.2.174 Certified-MS-Feature-List-For-GW

<b>WType-ID</b>	139 for Certified-MS-Feature-List-For-GW
<b>Description</b>	This attribute contains the Certified Feature indication for the MS to for the GW
<b>Value-Type</b>	Grouped
<b>Value</b>	

In a Request the AVP identifies the WiMAX Capabilities supported by the ASN or the HA. In an Answer, signals the options selected by the Diameter server.

Certified-MS-Feature-List-For-GW::= < AVP Header: TBD>

[ Certified-For-MCBCS ]

[ Certified-For-LBS ]

[ Certified-Compression ]

\* [ AVP ]

AVP	TLV Name	Request	Answer	Notes
459	Certified-For-MCBCS	0	0-1	If not present implies that the MS is not certified for any MCBCS features
460	Certified-For-LBS	0	0-1	If not present implies that the MS is not certified for any LBS features
461	Certified-Compression	0	0-1	If not present implies that the MS is not certified for any Compression features

#### 5.5.2.175 Certified-MS-Feature-List-For-BS

<b>WType-ID</b>	140 for Certified-MS-Feature-List-For-BS
-----------------	--



<b>Description</b>	This attribute contains the Certified Feature indication for the MS to for the BS
<b>Value-Type</b>	Grouped
<b>Value</b>	

In a Request the AVP identifies the WiMAX Capabilities supported by the ASN or the HA. In an Answer, signals the options selected by the Diameter server.

Certified-MS-Feature-List-For-GW::= < AVP Header: TBD>

[Certified-for-Scan-Capability]

[Certified-for-Security-Capability]

[Certified-for-ARQ-Capability]

\* [ AVP ]

AVP	TLV Name	Request	Answer	Notes
462	Certified-for-Scan-Capability	0	0-1	If not present implies that the MS is not certified for any Scan Capability features
463	Certified-for-Security-Capability	0	0-1	If not present implies that the MS is not certified for any Security Capability features
464	Certified-for-ARQ-Capability	0	0-1	If not present implies that the MS is not certified for any ARQ Capability features

#### 5.5.2.176 Certified-For-MCBCS

<b>WType-ID</b>	459 for Certified-For-MCBCS
<b>Description</b>	Indicates the MCBCS features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any MCBCS features.
<b>Value-Type</b>	4 octet OctetString The following one octet Bit-map represent the MCBS features that the MS is certified for: <ul style="list-style-type: none"> <li>• Bit-#0 - Certified_for_MCBCS-App</li> <li>• Bit #1 - Certified_for_MCBCS-DSx</li> </ul> All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

#### 5.5.2.177 Certified-For-LBS

<b>WType-ID</b>	460 for Certified-For-LBS
<b>Description</b>	Indicates the LBS features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any LBS features.

<b>Value-Type</b>	<p>4 octet OctetString</p> <p>The following one octet Bit-map represent the LBS features that the MS is certified for:</p> <ul style="list-style-type: none"> <li>• Bit-#0 - Certified_for_LBS-Control-Plane</li> <li>• Bit #1 - Certified_for_LBS-Hybrid</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>
-------------------	--

1 **5.5.2.178 Certified-Compression**

<b>WType-ID</b>	461 for Certified-Compression
<b>Description</b>	Indicates the Compression features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any Compression features.
<b>Value-Type</b>	<p>4 octet OctetString,</p> <p>The following one octet Bit-map represent the Compression features that the MS is certified for:</p> <ul style="list-style-type: none"> <li>• Bit-#0 - Certified_for_ROHC</li> <li>• Bit #1 - Certified_for_PHS</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

2 **5.5.2.179 Certified-Scan-Capability**

<b>WType-ID</b>	462 for Certified-Scan-Capability
<b>Description</b>	Indicates the Scan Capability features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any Scan Capability features.
<b>Value-Type</b>	<p>4 octet OctetString</p> <p>The following one octet Bit-map represent the Scan Capability features that the MS is certified for:</p> <ul style="list-style-type: none"> <li>• Bit-#0 – Certified for HO Scanning</li> <li>• Bit-#1 – Certified for Scan Report Type Support</li> <li>• Bit-#2 – Certified for HO/Scan/Report Trigger Metrics</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

3 **5.5.2.180 Certified-Security-Capability**

<b>WType-ID</b>	463 for Certified-Security-Capability
<b>Description</b>	Indicates the Security Capability features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any Security Capability features.
<b>Value-Type</b>	<p>4 octet OctetString</p> <p>The following one octet Bit-map represent the Security Capability features that the MS is certified for:</p> <ul style="list-style-type: none"> <li>• Bit-#0 – Certified for PKM message encoding support</li> <li>• Bit-#1 – Certified for Authorization policy support – Initial Network entry</li> <li>• Bit-#2 – Certified for Authorization policy support – Network re-entry</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

### 5.5.2.181 Certified-ARQ-Capability

<b>WType-ID</b>	464 for Certified-ARQ-Capability
<b>Description</b>	Indicates the ARQ Capability features that the MS is certified for. The absence of this attribute implies that the MS is not certified for any ARQ Capability features.
<b>Value-Type</b>	<p>4 octet OctetString</p> <p>The following one octet Bit-map represent the ARQ Capability features that the MS is certified for:</p> <ul style="list-style-type: none"> <li>• Bit-#0 – Certified for Sending and Receiving PDU for ARQ</li> <li>• Bit-#1 – Certified for ARQ feedback message</li> <li>• Bit-#2 – Certified for ARQ Discard message</li> <li>• Bit-#3 – Certified for ARQ Reset message</li> </ul> <p>All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.</p>

### 5.5.3 Reused Diameter AVPs

This chapter lists Diameter AVPs originally defined in other standards but reused by WiMAX. The description provides additional, WiMAX specific information in addition to the original definition of the referenced standards.

#### 5.5.3.1 Session-Id

<b>WType-ID</b>	263 for Session-Id as specified in [54]
<b>Description</b>	<p>The Session-Id AVP is used to identify a session pertaining to a specific anchored authenticator in WiMAX. The value is generated by NAS during access authentication and remains constant until anchor authenticator relocation. All authentication and accounting messages generated by a specific anchored authenticator MUST include only one Session-Id AVP and the same value MUST be used. The Session-Id MUST be globally and eternally unique, as it is meant to uniquely identify a user session at a specific time without reference to any other information, and may be needed to correlate historical authentication information with accounting information.</p>
<b>Value-Type</b>	UTF8String

#### 5.5.3.2 Acct-Session-Id

<b>WType-ID</b>	44 for Acct-Session-Id as specified in [54]
<b>Description</b>	<p>In WiMAX, the Acct-Session-Id AVP is used to match Start, Interims, and Stop messages that belong to the same accounting segment. It is generated by the accounting client and is unique per start/stop pair.</p> <p>Note: In WiMAX specific Diameter accounting application, this AVP is used even if the RADIUS/Diameter translation doesn't occur.</p>
<b>Value-Type</b>	OctetString

### 1 5.5.3.3 Acct-Multi-Session-Id

<b>WType-ID</b>	50 for Acct-Multi-Session-Id as specified in [54]
<b>Description</b>	In WiMAX, the Acct-Multi-Session-Id AVP contains the value of WiMAX-Session-Id which is generated by AAA after successful authentication / Re-authentication and delivered to the NAS in a Diameter-EAP-Answer message. It is unique per CSN and is used to match all accounting records within a session.
<b>Value-Type</b>	Unsigned32

### 2 5.5.3.4 Acct-Application-Id

<b>WType-ID</b>	259 for Acct-Application-Id as specified in [54]
<b>Description</b>	The Acct-Application-Id AVP contains the value of TBD defined for WiMAX offline charging application.
<b>Value-Type</b>	Unsigned32

### 3 5.5.3.5 NAS-IP-Address

<b>WType-ID</b>	4 for NAS-IP-Address as specified in [62]
<b>Description</b>	The NAS-IP-Address AVP contains the IPv4 address of the NAS/Accounting client providing service to the user. This value is used by AAA when generating Access-Network-Charging-Address AVP for the PCC-R3-OFC' interface.  Note: In WiMAX specific Diameter accounting application, this AVP is used even if the RADIUS/Diameter translation doesn't occur.
<b>Value-Type</b>	OctetString

### 4 5.5.3.6 NAS-IPv6-Address

<b>WType-ID</b>	95 for NAS-IPv6-Address as specified in [62]
<b>Description</b>	The NAS-IPv6-Address AVP contains the IPv6 address of the NAS/Accounting client providing service to the user. This value is used by AAA when generating Access-Network-Charging-Address AVP for the PCC-R3-OFC' interface.  Note: In WiMAX specific Diameter accounting application, this AVP is used even if the RADIUS/Diameter translation doesn't occur.
<b>Value-Type</b>	OctetString

### 5 5.5.3.7 Service-Context-Id

<b>WType-ID</b>	461 for Service-Context-Id as specified in [16]
<b>Description</b>	The Service-Context-Id AVP is defined in IETF RFC 4006 [16]. It contains a unique identifier of the Diameter Credit Control service specific document that applies to the request. This is an identifier allocated by the service provider/operator, by the service element manufacturer or by a standardization body and MUST uniquely identify a given Diameter Credit Control service specific document. For offline charging, this identifies the service specific document name and version on which associated CDRs should be based.
<b>Value-Type</b>	UTF8String  The format of the Service-Context-Id is:  "extensions".NAP.[NSP].Release."service-context" "@" "domain"

	<p>The WiMAX specific values for "service-context" "@" "domain" are:</p> <ul style="list-style-type: none"> <li>• WiMAX Charging doc#@wimaxforum.org</li> </ul> <p>The "Release" indicates the WiMAX Release the service specific document is based upon e.g. 1.5 for Release 1.5.</p> <p>As a minimum, Release "service-context" "@" "domain" SHALL be used. If the minimum is used all operator configurable parameters (Oc and Om) are optional.</p> <p>The NAP.[NSP] identifies the operator implementing the service specific document, which is used to determine the specific requirements for the operator configurable parameters.</p> <p>The "extensions" is operator specific information to any extensions in a service specific document.</p>
--	--

### 1 5.5.3.8 Multiple-Services-Credit-Control

<b>WType-ID</b>	456 for Multiple-Services-Credit-Control as specified in [63]
<b>Description</b>	The Multiple-Services-Credit-Control AVP is specified in IETF RFC 4006 [63] and extended by TS32.299 [99]. In case of PCC scenario, charging identifier from Application Function (AF) might be used by billing system to correlate charging data records for the same service, but generated in different layers. AF-Correlation-Information AVP [99] needs to be provided. See [3] for more details on this specific case.
<b>Value-Type</b>	Grouped

2

Multiple-Services-Credit-Control ::= < AVP Header: 456 >

- [ Granted-Service-Unit ]
- [ Requested-Service-Unit ]
- \* [ Used-Service-Unit ]
- ~~[ Tariff Change Usage ]~~
- \* [ Service-Identifier ]
- [ Rating-Group ]
- \* [ G-S-U-Pool-Reference ]
- [ Validity-Time ]
- [ Result-Code ]
- [ Final-Unit-Indication ]
- [ Time-Quota-Threshold ]
- [ Volume-Quota-Threshold ]
- [ Unit-Quota-Threshold ]
- [ Quota-Holding-Time ]
- [ Quota-Consumption-Time ]
- \* [ Reporting-Reason ]
- [ Trigger ]

~~{ PS-Furnish-Charging-Information }~~

\* ~~{ AF-Correlation-Information }~~ Only used in case of PCC. See [3] for further details.

\* ~~{ Envelope }~~

~~{ Envelope-Reporting }~~

[ Time-Quota-Mechanism ]

\* [ AVP ]

### 5.5.3.9 Access-Network-Charging-Identifier-Gx

<b>WType-ID</b>	1022 for Access-Network-Charging-Identifier-Gx as specified in [98]
<b>Description</b>	Access-Network-Charging-Identifier-Gx as specified in 3GPP TS29.212 [98]. The AVP contains the Access-Network-Charging-Identifier-Value. In WiMAX, Access-Network-Charging-Identifier-Value is PDFID. For pre-provisioned service flows, the A-PCEF/Accounting Client gets the PDFID from AAA during the access authentication. For dynamic service flows, the A-PCEF/Accounting Client generates the PDFID value when the packet data flow is established and sends it to PCRF in the CCR or RAA command during IP-CAN session establishment.
<b>Value-Type</b>	Grouped

Access-Network-Charging-Identifier-Gx ::= < AVP Header: 1022 >

{ Access-Network-Charging-Identifier-Value }

\* ~~{ Charging-Rule-Base-Name }~~ Only used in case of PCC. See [3] for further details.

\* ~~{ Charging-Rule-Name }~~ Only used in case of PCC. See [3] for further details.

### 5.5.3.10 Service-Information

<b>WType-ID</b>	873 for Service-Information as specified in [99]
<b>Description</b>	The purpose of the <i>Service-Information</i> AVP is to allow the transmission of additional 3GPP service specific information elements which are not described in this document. The format and the contents of the fields inside the Service-Information AVP are specified in the middle-tier documents which are applicable for the specific service. Note that the formats of the fields are service-specific, i.e. the format will be different for the various services. Further fields may be included in the Service-Information AVP when new services are introduced. For WiMAX access network charging, WiMAX-Information AVP is defined to be included in the Service-Information AVP.
<b>Value-Type</b>	Grouped

Service-Information ::= < AVP Header: 873 >

~~[ Subscription-Id ]~~  
~~[ PS-Information ]~~  
~~[ WLAN-Information ]~~  
~~[ IMS-Information ]~~  
~~[ MMS-Information ]~~  
~~[ LCS-Information ]~~  
~~[ PoC-Information ]~~  
~~[ MBMS-Information ]~~  
~~[ SMS-Information ]~~  
[ Service-Generic-Information ]  
[ WiMAX-Information ]

Only used in case of PCC. See [3] for further details.

1

## 2 5.5.3.11 Operator-Name

<b>WType-ID</b>	TBD by IETF for Operator-Name
<b>Description</b>	This attribute is defined in [96] and contains the country code and the WiMAX assigned company code of the role of the WiMAX operator.
<b>Value-Type</b>	UTF8String
<b>Value</b>	<p>The Text field is formatted as follows:</p> <pre> 0                               1                               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... +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+...   Namespace ID   Operator-Name +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+...   Operator-Name +---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+... </pre> <p>Where the Namespace ID is as defined by [96] with the value of 0x34 assigned by IANA to WiMAX.</p> <p>The Operator-Name field is of type Text and is defined by this specification to consist of 3 sub-fields as follows:</p> <p>The first sub-field consists of a single octet enumeration encoded in ASCII defining the role of the operator as follows:</p> <ul style="list-style-type: none"> <li>• “0” (0x30) Reserved</li> <li>• “1” (0x31) The operator role is a Visited NSP.</li> <li>• “2” (0x32) The operator role is a Home NSP.</li> <li>• All other values reserved.</li> </ul> <p>The second sub-field consists of 3 octets encoded in ASCII representing the ISO 3166-1 alpha-3 Country Code of the operator. The codes “WF1” and “WF2” SHALL be reserved</p>

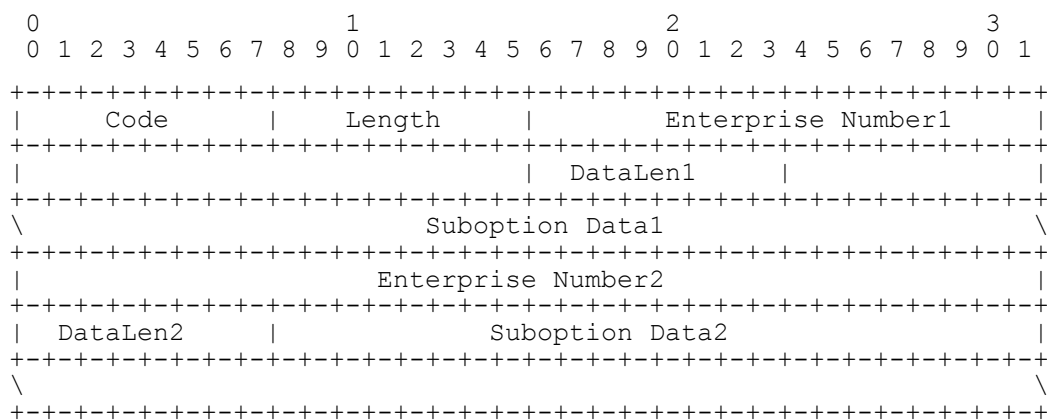
	<p>for Marine and Satellite operators respectively by the WiMAX Forum.</p> <p>The third sub-field consists of 3 octets encoded in ASCII representing the company codes assigned by the WiMAX Forum. This sub-field SHALL NOT contain an ISO 3166-1 alpha-3 Country Code and the WiMAX Forum reserved codes: “WF1” and “WF2”.</p>
--	--

## 5.6 DHCP Vendor Specific Options

### 5.6.1 WiMAX Radio Link Characteristics vendor specific option

This section describes how WiMAX radio link characteristics are mapped to a DHCP message as a vendor specific suboption.

The Vendor-Specific suboption takes the following form:



Code: 9 for the DHCP suboption

Length:  $\geq 4$

The one-byte Length field is the length of the data carried in the suboption, in bytes. The length includes the length of the first Enterprise Number; the minimum length is 4 bytes.

Enterprise Number1:

24757 the WiMAX Forum IANA entry

The value is a four-byte integer in network byte-order.

DataLenN:

The length of the data associated with the Enterprise Number.

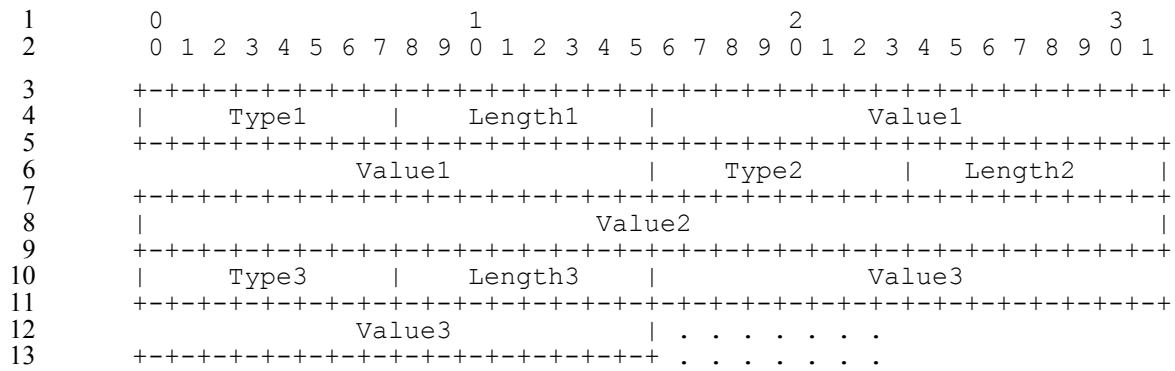
Suboption Data:

RFC4243 defines the Suboption as an opaque sequence of bytes allowing the Vendor to make use of the Suboptions to define its own specification.

### WiMAX Line Characteristics DHCP Vendor-Specific Suboption Data format

The sub option data format is shown below. The fields are transmitted from left to right. The WiMAX Line Characteristics are to be transmitted in a single request as multiple Type/Length/Values (TLVs).





14 TypeN:

15 The Type field is one octet. The following values are reserved for the type field and each is  
16 explained in a later section.

17 LengthN:

18 The one-byte Length field is the length of the data carried in the suboption, in bytes. The length is  
19 the length of the data carried in the Value.

20 ValueN:

21 The Value field is zero or more octets and contains information specific to the Attribute. The format  
22 and length of the Value field are determined by the Type and Length fields.

23

## 24 WiMAX Line Characteristics DHCP Type Definitions

DSL Line Characteristics DHCP Type Definition			
Type	Length	Value	Value type
0x81	4	Actual data rate upstream in kbs	32 bit unsigned integer
0x82	4	Actual data rate downstream in kbs	32 bit unsigned integer
0x83	4	Minimum Data Rate Upstream in kbs	32 bit unsigned integer
0x84	4	Maximum Data Rate Upstream in kbs	32 bit unsigned integer
0x87	4	Maximum Data Rate Upstream in kbs	32 bit unsigned integer
0x88	4	Minimum Data Rate Upstream in kbs	32 bit unsigned integer

## 5.7 IP Mobility Messages

### 5.7.1 PMIP6 Messages

This section provides definition for IP mobility messages utilized by Proxy Mobile IPv6 (PMIP6) feature over the R3 reference point, between the Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA) network entities.

#### 5.7.1.1 PBU and PBA messages

Table 5-47 defines required and optional contents, definition of field and mobility option values, for the Proxy Binding Update (PBU) and Proxy Binding Acknowledgement (PBA) messages exchanged between the MAG and the LMA.

**Table 5-47 – PBU/PBA Fields and Options**

Fields and (>) Options	Type	Description	PBU	PBA
Sequence Number	N/A	Per MN's mobility session specific number. In the PBA set to the value received from the corresponding PBU.	1	1
Lifetime	N/A	Set to the requested number of time units the binding SHALL remain valid. If set to 0, requests deletion of the BCE.	1	1
Acknowledge (A)	N/A	Set to "1" to request an acknowledgement message.	1	0
Proxy Registration Flag (P)	N/A	Set to "1" to indicate that the Binding Update message is a proxy registration.	1	1
Status	N/A	Set to indicate the result as specified in RFC 3775 [57].	0	1
> Mobile Node Identifier option	8	Set to the MN-NAI	1 [c]	1
> Home Network Prefix option	22	For dynamic allocation, set to the value "0::/0" (ALL_ZERO value) to request allocation for the MS's connection of an IPv6 Home Network Prefix. For static allocation, the MAG sets the value to the previously allocated IPv6 Home Network Prefix.  When present in the PBA carries the HNP assigned to the MS.	0-1 [a]	0-1 [a]
> Handoff Indicator option	23	An 8-bit field that specifies the type of handoff. The values (0 – 255) will be allocated and managed by IANA. The following values are currently defined.  0: Reserved  1: Attachment over a new interface	1 [b]	1 [b]

		<p>2: Handoff between two different interfaces of the mobile node</p> <p>3: Handoff between mobile access gateways for the same interface</p> <p>4: Handoff state unknown</p> <p>5: Handoff state not changed (Re-registration)</p>		
> Access Technology Type option	<b>24</b>	Set to value 5 for the WiMAX access type	1	1
> Timestamp option	<b>27</b>	Set to the current time	1	1
> GRE key option	<b>TBD</b>	Set to the downlink GRE key to be used for downlink GRE encapsulated packets	0-1	0-1
> IPv4 Home Address option	<b>TBD</b>	For dynamic allocation, set to the value "0.0.0.0" to request allocation for the MS's connection of an IPv4 Home Address. For static allocation, the MAG sets the value to the previously allocated IPv4 Home Address	0-1 [a]	0
> IPv4 Address Acknowledgement option	<b>TBD</b>	Carries the IPv4 HoA assigned to the MS, (either the value from PBU if one provided, or the IPv4 HoA allocated by the LMA)	0	0-1 [a]
> IPv4 Default-Router Address Option	<b>TBD</b>	Set to the MS's IPv4 default router address. This option SHALL be present if and only if IPv4 Home Address option is present in the PBA.	0	0-1
> Link-local Address Option	<b>26</b>	<p>If populated in the PBU it carries the Link-local address of the MAG indicated to the LMA.</p> <p>In the PBA: valid link-layer address for this session to be used by the MAG (generated by LMA or retrieved from the BCE).</p>	<b>0-1</b>	0-1
> MN-HA Mobility Message Authentication Option	<b>9/1</b>	This option has the information to authenticate the relevant mobility entity.	<b>0-1</b>	0-1

**Notes:**

- [a] At least one of the two options, namely, the IPv6 Home Network Prefix option or the IPv4 Home Address option SHALL be present. Providing more than one of the options, IPv6 Home Network Prefix(es) and the IPv4 Home Address, in the PBU or PBA message is out of scope.
- [b] Handoff indicator value 2 is not used in this release of the specification.
- [c] Value of the MN ID option in the PBU SHALL be set to PMIP-Authenticated-Network-Identity value when it is available to the MAG. In case it is not available, the Outer-Identity used during initial network entry of the MS SHALL be utilized instead.

### 5.7.1.2 BRI and BRA messages

Table 5-48 defines required and optional contents, definition of field and mobility option values, for the Binding Revocation Indication (BRI) and Binding Revocation Acknowledgement (BRA) messages exchanged between the MAG and the LMA.

**Table 5-48 – BRI/BRA Fields and Options**

Fields and (>) Options	Type	Description	BRI	BRA
Sequence Number	N/A	A sequence number generated by the LMA, and increased for every BRI sent.  Set to the value received in the corresponding BRI.	1	1
Revocation Trigger	N/A	Set to a value indicating the event which triggered the revoking node to send the BRI message	1	0
Proxy Binding Flag (P)	N/A	Set to "1" to indicate that the Binding Revocation Indication is for a proxy MIP6 binding entry.	1	1
Acknowledge (A)	N/A	Set to "1" to request an acknowledgement message.	1	0
Global Per-Peer Bindings (G)	N/A	Set to 0 to indicate that the request is for a specific PMIP6 BCE.	1	1
Status	N/A	Indicates the result of the BRI: can be set to 0 for success, 1 for an unspecified failure or 2 for an inexistent MS binding.	0	1
> Mobile Node Identifier option	8	Set to the MN-NAI in BRI.  Copied from corresponding field of BRI in BRA.	1	1
> IPv6 Home Network Prefix option	22	Set to the Home Network Prefix of the MS's connection.	0-1 [a]	0-1 [a]
>IPv4 Home Address option	TBD	Set to the IPv4 home address of the MS's connection.	0-1 [a]	0
> IPv4 Address Acknowledgement option	TBD	Set to the IPv4 address of the MS's connection indicated in BRI	0	0-1 [a]
> MN-HA Mobility Message Authentication Option	9/1	This option has the information to authenticate the relevant mobility entity.	0-1	0-1

**Notes:**

- [a] At least one of the two options, namely, the IPv6 Home Network Prefix option or the IPv4 Home Address option SHALL be present. Providing more than one of the options, IPv6 Home Network Prefix(es) and the IPv4 Home Address, in the BRI or BRA message is out of scope.

## 5.8 TLV Definitions for EAP-Notification

### 5.8.1 Notification-Information

<b>Type</b>	1 for Notification-Information		
<b>Length in octets</b>	Variable		
<b>Description</b>	The Notification Information is coded as follows:		
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>Description</b>	<b>M/O</b>
	Notification Code	Identifies the type of notification	O
	Mobility Access Classifier	Must be present for notification code 0xF000.	O
	Allowed Location Information	BS ID List where a fixed or nomadic MS is allowed network entry.	O

Note: Due to the limitations imposed by the EAP-Notification message transport the total payload SHALL NOT exceed 1015 Octets includes the Network Rejection Information fields.

### 5.8.2 Notification-Code

<b>Type</b>	2 for Notification-Code
<b>Length in octets</b>	4
<b>Value</b>	32-bit unsigned integer.
<b>Description</b>	Time for MAG-LMA-PMIP6 key remaining valid. This is provided to the MAG by the anchor Authenticator for PMIP6 key context transfer.
<b>Parent TLV(s)</b>	<b>Notification-Information</b>

### 5.8.3 Network Rejection Information

<b>Type</b>	3 for Network Rejection Information		
<b>Length in octets</b>	Variable		
<b>Description</b>	The Network Rejection Information is coded as follows:		
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>Description</b>	<b>M/O</b>
	Rejection Code		M
	Received NAI		M
	Emergency Services Override		O
	Allowed Location Information		O
	RMAC (Rejection Message Authentication Code) Value		M

Note: Due to the limitations imposed by the EAP-Notification message transport the total payload SHALL NOT exceed 1015 Octets includes the Network Rejection Information fields.

#### 1 5.8.4 Rejection Code

<b>Type</b>	4 for Rejection Code
<b>Length in octets</b>	2
<b>Value</b>	<p>The Rejection Code value is defined as follows:</p> <p><b>Rejection Class A</b> – Rejection Codes in the range 0x0000 – 0x00FF</p> <ul style="list-style-type: none"> <li>• 0x0000 = Rejection Class A – General Error</li> <li>• 0x0001 = Invalid Subscription Information</li> <li>• 0x0002 = Major Network Problem</li> <li>• 0x0003 = Unpaid Bills</li> <li>• 0x0004 = Illegal Mobile Equipment</li> <li>• 0x0005 = Device Type not supported by NSP</li> <li>• 0x0006 = Misbehaving MS Equipment</li> </ul> <p>All other Rejection codes in Rejection Class A are undefined.</p> <p><b>Rejection Class B</b> – Rejection Codes in the range 0x0100 – 0x01FF</p> <ul style="list-style-type: none"> <li>• 0x0100 = Rejection Class B – General Error</li> <li>• 0x0101 = No Roaming Agreement existing with the Home or the Visited Network</li> <li>• 0x0102 = Illegal Mobile Equipment</li> <li>• 0x0103 = Device Type not supported by NSP</li> <li>• 0x0104 = Invalid Subscription/Configuration</li> <li>• 0x0105 = Misbehaving MS Equipment</li> </ul> <p>All other Rejection codes in Rejection Class B are undefined.</p> <p><b>Rejection Class C</b> – Rejection Codes in the range 0x0200 – 0x02FF</p> <ul style="list-style-type: none"> <li>• 0x0200 = Rejection Class C – General Error</li> <li>• 0x0201 = Invalid Subscription Information</li> <li>• 0x0202 = Major Network Problem</li> <li>• 0x0203 = Unpaid Bills</li> <li>• 0x0204 = Illegal Mobile Equipment</li> <li>• 0x0205 = Device Type not supported by NSP</li> <li>• 0x0206 = Misbehaving MS Equipment</li> </ul> <p>All other Rejection codes in Rejection Class C are undefined.</p> <p><b>Rejection Class D</b> – Rejection Codes in the range 0x0300 – 0x03FF</p> <ul style="list-style-type: none"> <li>• 0x0300 = Rejection Class D – General Error</li> <li>• 0x0301 = No Roaming Agreement existing with the Home or the Visited Network</li> <li>• 0x0302 = Illegal Mobile Equipment</li> <li>• 0x0303 = Device Type not supported by NSP</li> <li>• 0x0304 = Invalid Subscription/Configuration</li> <li>• 0x0305 = Misbehaving MS Equipment</li> </ul> <p>All other Rejection codes in Rejection Class D are undefined.</p>

	<p><b>Rejection Class E</b> – Rejection Codes in the range 0x0400 – 0x04FF</p> <ul style="list-style-type: none"> <li>• 0x0400 = Rejection Class E – General Error</li> <li>• 0x0401 = Temporary Network Problem at H-NSP</li> </ul> <p>All other Rejection codes in Rejection Class E are undefined.</p> <p><b>Rejection Class F</b> – Rejection Codes in the range 0x0500 – 0x05FF</p> <ul style="list-style-type: none"> <li>• 0x0500 = Rejection Class F – General Error</li> <li>• 0x0501 = No Roaming Agreement existing with the Home or the Visited Network</li> <li>• 0x0502 = Temporary Network Problem at V-NSP</li> </ul> <p>All other Rejection codes in Rejection Class F are undefined.</p> <p><b>Rejection Class G</b> – Rejection Codes in the range 0x0600 – 0x06FF</p> <ul style="list-style-type: none"> <li>• 0x0600 = Rejection Class G – General Error</li> <li>• 0x0601 = Access outside defined Service Area</li> </ul> <p>All other Rejection codes in Rejection Class G are undefined.</p> <p><b>Rejection Class H</b> – Rejection Codes in the range 0x0700 – 0x07FF</p> <ul style="list-style-type: none"> <li>• 0x0700 = Rejection Class H – General Error</li> <li>• 0x0701 = No Roaming Agreement existing with the Home or the Visited Network</li> <li>• 0x0702 = Access outside defined Service Area</li> </ul> <p>All other Rejection codes in Rejection Class H are undefined.</p> <p><b>Rejection Class I</b> – Rejection Codes in the range 0x0800 – 0x08FF</p> <ul style="list-style-type: none"> <li>• 0x0800 = Rejection Class I – General Error</li> <li>• 0x0801 = MS equipment not compliant with V-NSP</li> </ul> <p>All other Rejection codes in Rejection Class I are undefined.</p> <p><b>Rejection Class J</b> – Rejection Codes in the range 0x0900 – 0x09FF</p> <ul style="list-style-type: none"> <li>• 0x0900 = Rejection Class J – General Error</li> <li>• 0x0901 = MS equipment not compliant with V-NSP</li> </ul> <p>All other Rejection codes in Rejection Class J are undefined.</p> <p><b>Rejection Class K</b> – Rejection Codes in the range 0x0A00 – 0x0AFF</p> <ul style="list-style-type: none"> <li>• 0x0A00 = Rejection Class K – General Error</li> <li>• 0x0A01 = MS equipment not compliant with H-NSP</li> </ul> <p>All other Rejection codes in Rejection Class K are undefined.</p> <p>All other values are reserved and SHALL be treated as if receiving Rejection Code 0x0000.</p>
<b>Description</b>	

### 1 5.8.5 Allowed Location Information

<b>Type</b>	5 for Allowed Location Information		
<b>Length in octets</b>	Variable		
<b>Elements (Sub-TLVs)</b>	<b>TLV Name</b>	<b>Description</b>	<b>M/O</b>
	BS ID	Allowed BS #1	O
	BS ID	Allowed BS #2	O
	...	...	...
	BS ID	Allowed BS #n	O
<b>Description</b>	The Allowed Location Information may be used as a hint by the MS		

### 2 5.8.6 Received NAI

<b>Type</b>	6 for Received NAI
<b>Length in octets</b>	Variable
<b>Value</b>	<p>The NAI as received from the MS in the EAP-Identity/Response message during network access authentication and authorization. The NAI is mirrored by the Authenticator to allow the MS to detect any modification of the NAI and especially the realm portion or routing decoration originally used by the MS in the (unprotected) EAP-Identity/Response message over-the-air.</p> <p>UTF-8 encoded string without the null character representing the NAI as defined by RFC 4282</p>
<b>Description</b>	

### 3 5.8.7 Emergency Services Override

<b>Type</b>	7 for Emergency Services Override
<b>Length in octets</b>	1
<b>Value</b>	<p>Unsigned Octet. Supported values:</p> <p>0x0000 = Emergency Services Override not supported.</p> <p>0x0001 = Emergency Services Override supported</p> <p>All other values are reserved, and SHALL be treated as if the Emergency Services Override TLV was not present.</p>
<b>Description</b>	<p>If the MS receives network rejection information with the Emergency Services Override TLV with a value identifying not supported, it SHALL treat this as a hint that whilst the Rejection Duration/Criteria has not been met, the rejection will hold even if the MS attempts an emergency network entry.</p> <p>If the MS receives network rejection information with the Emergency Services Override TLV with a value identifying supported, it SHALL treat this as a hint that whilst the Rejection Duration/Criteria has not been met, the MS attempting an emergency network entry may succeed.</p> <p>The Home AAA SHALL NOT send the Emergency Service Override set to “not supported” when the MS is roaming.</p>



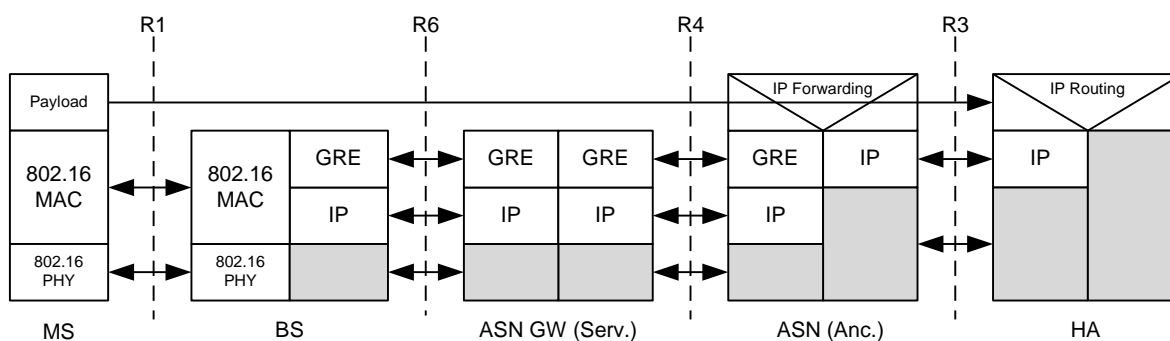
### 1 5.8.8 RMAC (Rejection Message Authentication Code) Value

<b>Type</b>	8 for RMAC (Rejection Message Authentication Code) Value
<b>Length in octets</b>	32
<b>Value</b>	<p>32 octet RMAC Value SHALL be generated from the EMSK using the following formula:</p> $\text{RMAC-Value} = \text{HMAC-SHA256}(\text{RMAC Key}, \text{Network Rejection Information TLV})$ <p>where:</p> $\text{RMAC-1} = \text{HMAC-SHA256}(\text{EMSK}, \text{usage-data} \parallel 0x01)$ $\text{RMAC-2} = \text{HMAC-SHA256}(\text{EMSK}, \text{RMAC-1} \parallel \text{usage data} \parallel 0x02)$ $\text{RMAC-Key} = \text{RMAC-1} \parallel \text{RMAC-2}$ <p>where:</p> <p>usage-data = key label + "\0" + length</p> <p>key label = rmac-key@wimaxforum.org in ASCII</p> <p>length = 0x0200 the length in bits of the RMAC-Key expressed as a 2 byte unsigned integer in network order.</p> <p>RMAC-Value is a 32 octet HMAC-SHA256 digest value, where the RMAC-Key is used for the key and the whole Network Rejection Information TLV is used for the data, except that the value field of the RMAC Value TLV included in the Rejection Information is set to zero when calculating the RMAC-Value. After calculation, the value field of the RMAC Value TLV included in the Network Rejection Information TLV is replaced with the calculated RMAC-Value.</p>
<b>Description</b>	

## 6. Data Plane

The data plane consists of the transport encapsulation of the user payload within the mobile WiMAX network. Basic considerations are provided in chapter 7.11 of the Stage 2 documentation. Stage 3 section 6 amends the Stage 2 description by providing detailed information on the applied protocols.

In the current Release of the mobile WiMAX network specification assumes a routed transport infrastructure for all of the exposed network reference points. Therefore user payload packets are encapsulated within IP packets when they are carried over the reference points R3, R4 and R6. User payload packets are encapsulated in 802.16 MAC frames when carried over R1.



**Figure 6-1 – Data Plane with R4 and R6**

If the payload contains Ethernet framing, Ethernet frames coming from R1 SHALL NOT be terminated before the (anchor) ASN.

No dedicated data plane protocol is specified for R2 or R5. User payload is transferred without any encapsulation according to the source and destination addresses in the user payload packets.

### 6.1 Encapsulation on R3

#### 6.1.1 IP in IP Encapsulation

According to [48] IP-in-IP encapsulation SHALL be applied for transport of user payload over the reference point R3. The encapsulation SHALL be done in accordance to RFC2003. Reverse tunneling SHALL be done according to RFC3024.

If PMIP6 is used as the mobility protocol providing services to the MS, the transport used over R3 reference point may be either IPv6 or IPv4. The IPv6-in-IPv6 encapsulation on an IPv6-based R3 reference point SHALL be supported, as specified in RFC2473 [28]. For transport of IPv6 packets over an IPv4-based R3, the encapsulation mode could be either IPv6 in IPv4 directly, IPv6 in IPv4 UDP or IPv6 in IPv4 UDP TLV and is negotiated between the MAG and the LMA as per [93]. To support interoperability, IPv6 in IPv4 direct encapsulation SHALL be supported by both MAG and LMA.

When IPv4 transport is used in PMIP6 service, the MAG is still required to have an IPv6 address as per [93]. This IPv6 address must be global unique, and could be either IPv6 global unicast address (RFC3587 [53]), Unique Local IPv6 unicast address (RFC4193[67]) or IPv4-mapped IPv6 address (RFC4291 [72]). How to assign this IPv6 address is outside the scope of this specification.

#### 6.1.2 GRE Encapsulation

As an option in [48], GRE (Generic Route Encapsulation) encapsulation MAY be applied for transport of user payload over the reference point R3. GRE is specified in RFC2784 and extended in RFC2890 by the Key option as

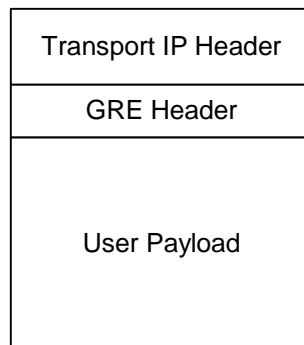
well as the Sequence Number option. When GRE encapsulation on R3 reference point is established through PMIP6 mobility signaling, the GRE negotiation and key management SHALL be performed as per [94].

### 6.1.3 Other Encapsulation

For Simple IP and Simple Ethernet other encapsulation protocols MAY be used. Details are out of scope.

## 6.2 GRE Encapsulation on R4 and R6

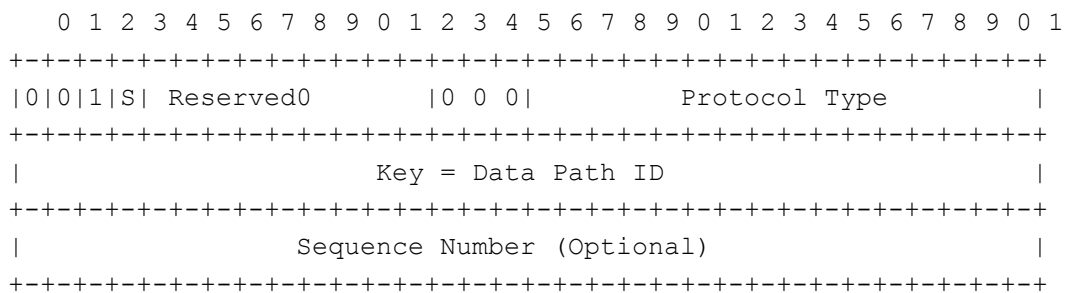
GRE as specified by [36] and extended by [41] SHALL be used as the tunneling protocol for the data plane over the reference points R4 and R6. GRE allows for tunneling of IP packets, Ethernet frames as well as WiMAX specific payload frames over an IP-based transport infrastructure. The same encapsulation protocol is applied on R4 and R6, regardless of the type of user payload, i.e., IPv4, IPv6, IPv4oETH, IPv6oETH, plain Ethernet or WiMAX specific payload frames, and regardless of the granularity of the tunnel, i.e., per service flow granularity.



**Figure 6-2 – GRE Encapsulation**

The GRE protocol according to [36] SHALL be used without the Checksum option. Therefore the Checksum Present bit is set to zero.

[41] provides two optional extensions, the Key option as well as the Sequence Number option. While the Key option SHALL be applied on R4 and R6 for providing the Data Path ID of the tunnel, the Sequence Number option MAY be provided for handover optimizations. When present, the Sequence Number field is signaled by the 'Sequence Number Present' bit in the GRE header.



**Figure 6-3 – GRE Header Format**

**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 <a href="http://www.iana.org/assignments/ethernet-numbers">http://www.iana.org/assignments/ethernet-numbers</a> : <ul style="list-style-type: none"> <li>IPv4: 0x0800</li> <li>IPv6: 0x86DD</li> <li>Ethernet: 0x6558</li> <li>For the WiMAX Payload Type, 0xFFFF SHALL be used.</li> </ul>
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'.

WiMAX Payload Type may be used to indicate if the upper protocol is PHS suppressed, ROHC compressed or uncompressed IP packet.

### 6.3 Convergence Sublayer on R1

IEEE802.16 Convergence Sublayer SHALL be located in the Anchor Data Path Function of ASN-GW. IEEE802.16 Convergence Sublayers SHALL be applied to the particular user payload for encapsulation and transport over R1.

Since the downlink packet classification of IEEE802.16 is taking place in the ASN-GW, the BS maps each Data Path ID into a particular MSID and SFID. In this case the mapping table in the BS is established and maintained by the Data Path Function. The uplink packet classification is taking place in the MS.

#### 6.3.1 IP-CS

IP datagrams going upstream over R1 are encapsulated in the BS as user payload in GRE packets and transferred over R6 and eventually R4 to the anchor ASN-GW/ASN. IP datagrams send downstream from the anchor ASN-GW within the payload of GRE packets are extracted in the BS out of the GRE packet and forwarded over R1 to the MS. All datagrams transferred upstream over R1 SHOULD be forwarded over R6, and all packets transferred downstream over R6 SHOULD be forwarded over R1. IP-CS here refers to both IPv4 and IPv6 types of datagrams, where the classifications rules are used to differentiate and map the specific IP transport connections over R1 and R6 reference points.

#### 6.3.2 IPoETH-CS

Ethernet frames going upstream over R1 are encapsulated in the BS as user payload in GRE packets and transferred over R6 and eventually R4 to the anchor ASN-GW/ASN. Ethernet frames send downstream from the anchor ASN-GW within the payload of GRE packets are extracted in the BS out of the GRE packet and forwarded over R1 to the MS. All Ethernet frames transferred upstream over R1 SHOULD be forwarded over R6, and all frames transferred downstream over R6 SHOULD be forwarded over R1.

Ethernet behavior in the user plane SHALL be realized by a multiport bridge in the anchor ASN-GW/ASN with a single port for each of the MSs. Ethernet frames are extracted out of the GRE packets before forwarding the frames into the particular bridge port. To allow DataPathID based identification of particular port. The granularity of the GRE tunnels over R4 or R6 SHALL NOT be per-BS. The MSs are connected to radio side ports of the bridge while the FA/Access Router is connected to a network side port of the bridge.

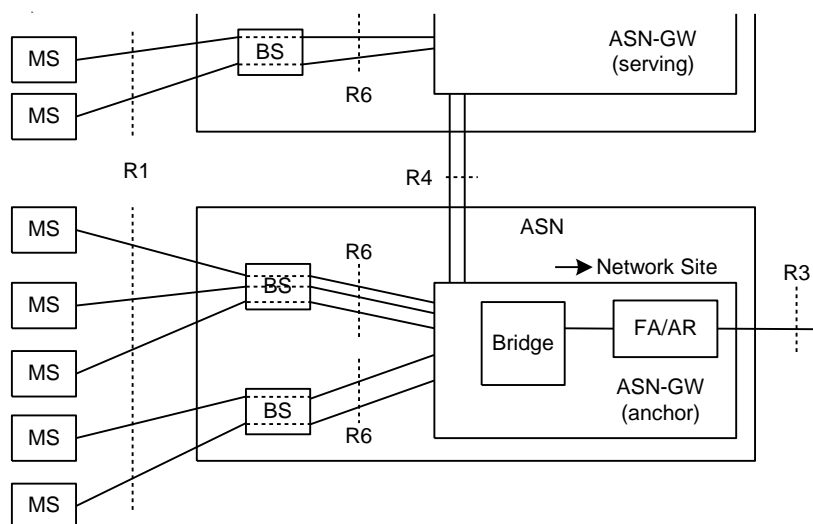
Downstream Ethernet frames coming out of bridge ports are encapsulated as user payload in GRE packets and forwarded over R6 or R4 towards the MS belonging to the port of the bridge. If multiple CIDs exist in downstream

for a particular MS, classification SHALL be performed in the scope of the CIDs belonging to the MS. Classification takes place in the (anchor) ASN/GW before encapsulating the Ethernet frames in GRE packets for per-SF granularity, of the GRE tunnels. After a handover the tunnels MAY be extended over R4 from the anchor ASN-GW/ASN to the serving ASN-GW/ASN.

Forwarding and processing of the Ethernet frames in the bridge SHALL be performed according to [IEEE802.1D] amended by [IEEE802.16k]. All multicast and multicast control messages SHALL be processed in the bridge according to [75]. Broadcasting messages to all radio side ports of the bridge and direct host-to-host communication between radio side ports of the bridge SHOULD be prevented.

Further information about processing of multicast and broadcast messages in such a bridge can be found in [83].

Figure 6-4 shows the adoption of the IPoETH-CS link model for the mobile WiMAX network architecture.



**Figure 6-4 – IPoETH-CS Link Model in the WiMAX Architecture**

### 6.3.3 ETH-CS

Ethernet frames going upstream over R1 are encapsulated in the BS as user payload in GRE packets and transferred over R6 and eventually R4 to the anchor ASN-GW/ASN. Ethernet frames sent downstream from the anchor ASN-GW within the payload of GRE packets are extracted in the BS out of the GRE packet and forwarded over R1 to the MS. All Ethernet frames transferred upstream over R1 SHOULD be forwarded over R6, and all frames transferred downstream over R6 SHOULD be forwarded over R1.

Downstream Ethernet frames coming out of the L2FW in the ASN-GW are encapsulated as user payload in GRE packets and forwarded over R6 or R4 towards the MS. If multiple CIDs exist in downstream for a particular MS, classification SHALL be performed in the scope of the CIDs belonging to the MS. Classification takes place in the (anchor) ASN/GW before encapsulating the Ethernet frames in GRE packets for per-SF granularity, of the GRE tunnels. After a handover the tunnels MAY be extended over R4 from the anchor ASN-GW/ASN to the serving ASN-GW/ASN.

## 7. Feature List for NWG Rel 1.5

Table 7-1 captures implementation requirements for various features supported in NWG Rel 1.5. This table lists aspects of the NWG Release 1.5 specification where two or more solution alternatives are implied and summarizes Mandatory/default and optional choices for implementation of SS/MS, BS, ASN-GW, AAA and HA/LMA entities.

### Legend:

M – Mandatory, O – Optional, CM – Conditional Mandatory, NA – Not Applicable

“Mandatory” means that the feature is mandatory-to-implement, unless otherwise stated.

**Table 7-1 – Feature list for NWG Rel 1.5**

Feature	Implementation Requirements (SS/MS)	Implementation Requirements (BS)	Implementation Requirements (ASN-GW)	Implementation Requirements (AAA)	Implementation Requirements (HA/LMA)
Network Discovery and Selection - Manual and Automatic selection	M – Manual selection M – Automatic selection	NA	NA	NA	NA
Network Discovery and Selection – NAP and NSP Selection	M – NAP ID M – NSP ID NOTE: NAP and NSP IDs may be same or different. One or more NSP IDs may be advertised.	M – NAP ID M – NSP ID NOTE: NAP and NSP IDs may be same or different. One or more NSP IDs may be advertised.	M – NAP ID M – NSP ID NOTE: NAP and NSP IDs may be same or different. One or more NSP IDs may be advertised.	NA	NA
Network Discovery and Selection – NAP and NSP ID Format	M – 24-bit globally unique ID in MCC/MNC format  O – 24-bit ID from operator public ID pool <b>Note: need to add references.</b> NOTE: NAP and NSP IDs may be represented in either format	NA	M – 24-bit globally unique ID in MCC/MNC format  O – 24-bit ID from operator public ID pool NOTE: NAP and NSP IDs may be represented in either format	NA	NA
Convergence Sub layer	M – IPv4 CS O – IPv6 CS O – Ethernet CS Note: In TWG profile IPv6 CS is mandatory	NA	M – IPv4 CS O – IPv6 CS O – Ethernet CS	NA	NA
SS/MS – ASN OTA header suppression / compression	O – PHS O – ROHC NOTE: In TWG profile PHS and ROHC is Mandatory in MS/SS	O – PHS Note: In TWG profile PHS and ROHC is Mandatory in BS	O – PHS O – ROHC	NA	NA

EAP method for SS/MS device authentication	M: EAP-TLS  Note: EAP-TLS can also be used for subscription authentication.	NA	NA	M: EAP-TLS	NA
EAP method for SS/MS subscription authentication	O – EAP-TTLS O – EAP-AKA  NOTE: At least one shall be supported.	NA	NA	O – EAP-TTLS O – EAP-AKA  NOTE: At least one SHALL be supported. Both SHOULD be supported.	NA
ASN – CSN Authentication & Authorization protocol	NA	NA	M – RADIUS O – DIAMETER	M – RADIUS O – DIAMETER	NA
Offline Accounting models & protocols	NA	NA	If RADIUS is used for authentication and authorization: M (to use) – RADIUS offline  If Diameter is used for authentication and authorization: M (to use) – Diameter offline	If RADIUS is used for authentication and authorization: M (to use) – RADIUS offline  If Diameter is used for authentication and authorization: M (to use) – Diameter offline	O – Diameter offline O – RADIUS offline (Accounting support is optional in HA)
Online Accounting models & protocols	NA	NA	O – Diameter online O – RADIUS online	O – Diameter online O – RADIUS online	O – Diameter online O – RADIUS online
Accounting - Charging models	NA	NA	M – Volume based M – Time based	M – Volume based M – Time based	O – Volume based O – Time based (if accounting is supported on the HA, then the HA shall support volume based and time based accounting)
Accounting Granularity	NA	NA	M – IP Session based O – Flow based	M – IP Session based O – Flow based	O – IP session based
Accounting - Hotlining	NA	NA	O – RADIUS Based	O – RADIUS Based	O – RADIUS Based
QoS and Service Flow management	M – Network Initiated SF O – MS Initiated SF	NA	M – Pre-provisioned QoS with Network Initiated SF O – MS Initiated SF	NA	NA

QoS granularity	M – Per Service Flow (SF) granularity	M – Per SS/MS SF granularity	M – Per SS/MS SF granularity	NA	NA
HO Initiation	M – Client Initiated M – Network Initiated	M – Client Initiated M – Network Initiated	NA	NA	NA
HO Type	M – Predictive (controlled) and unpredictable (uncontrolled) HO	M – Predictive (controlled) and unpredictable (uncontrolled) HO	NA	NA	NA
MS IP Addressing – v4	For PMIPv4: M – DHCPv4 For CMIPv4: HoA delivered via CMIPv4 procedure	NA	For PMIPv4: M – DHCPv4 For CMIPv4: M – HA assigned	For PMIPv4, CMIPv4: M – Dynamic home address (HoA) assignment Note: Address assignment can be via HA, DHCPv4 or AAA	For PMIPv4, CMIPv4: M – Dynamic home address (HoA) assignment Note: Address assignment can be via HA, DHCPv4 or AAA
MS IP Addressing – v6	M – Stateless auto configuration O – DHCPv6	NA	M – Stateless auto configuration O – DHCPv6	PMIPv6/CMIPv6: M – dynamic home network prefix assignment  Simple-IP: dynamic prefix assignment	PMIPv6/CMIPv6: M – dynamic home network prefix assignment  Simple-IP: dynamic prefix assignment
IM/Paging - Announce	M – 802.16e paging primitives	NA	M – Topologically unaware O – Topologically aware	NA	NA
IM/Paging – R6 transport mechanism for Announce	NA	NA	O – IP Multicast M – IP Unicast	NA	NA
IM/Paging - PC relocation	NA	NA	O	NA	NA
IM/Paging - FA relocation	NA	NA	O	NA	NA
RRM	NA	O	O Note: only covers the relay functionality	NA	NA
CSN Anchored MM Protocol (MIP based)	O – CMIPv4 O – CMIPv6	NA	O – CMIPv4 O – CMIPv6 M – PMIPv4 O – PMIPv6	NA	M – MIPv4 O – CMIPv6 O – PMIPv6 Note: For MIPv4 HA is not aware of whether PMIP or CMIP is used.
R3 Tunneling	NA	NA	M – IP-in-IP O – GRE	NA	M – IP-in-IP O - GRE
DHCP (Ethernet Services)	NA	NA	M – L2 DHCP Relay (Ethernet Services only)	NA	NA



DHCP (Simple-IP)	M – DHCPv4 Client O – DHCPv6 Client	NA	M – DHCP Proxy O – DHCP Relay	NA	NA
DHCP (MIP- based CSN Anchored mobility)	M – DHCPv4 Client O – DHCPv6 Client	NA	M – DHCP Proxy O – DHCP Relay	NA	NA

1

