WiMAX Forum® Network Architecture

Detailed Protocols and Procedures

Base Specification

WMF-T33-001-R020v01
WMF Approved

(2012-04-17)

WiMAX Forum Proprietary

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

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.

Table of Contents

List of Figures

List of Tables

1. Introduction and Scope

This document describes the detailed procedures, call flows, messages, timers, TLVs and attributes for the WiMAX® end-to-end Network Architecture 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 1.6 of the WiMAX Forum® Network Architecture specification. In this Release, the specification covers stationary and mobile WiMAX® clients connecting to a mobile WiMAX network. The specification is based on WiMAX Forum Network Architecture Stage 1 requirements. This document is the basis for network interoperability test 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] WMF-T32-001-R016, WiMAX Forum® Network Architecture - Architecture Tenets, Reference Model and Reference Points – Base Specification

[2] WMF-T33-004-R010, WiMAX Forum® Network Architecture, Informative Annex: Hooks and Principles for Evolution (informative)

[3] WMF-T33-109-R016, WiMAX Forum®Network Architecture, Policy and Charging Control

[4] WMF-T31-001-R015, WiMAX Forum® Network Requirements, Recommendations and Requirements for Networks based on WiMAX Forum Certified® Products

[5] WMF-T33-102-R015, WiMAX Forum® Network Architecture, Emergency Services Support

[6] WMF-T33-103-R016, WiMAX Forum® Network Architecture, Architecture, detailed Protocols and Procedures, WiMAX® Over-The-Air General Provisioning System Specification

[7] WMF-T33-104-R016, WiMAX Forum® Network Architecture, Detailed Protocols and Procedures, WiMAX® Over-The-Air Provisioning & Activation Protocol based on OMA DM Specifications

[8] WMF-T33-108-R015, WiMAX Forum® Network Architecture, Robust Header Compression (ROHC) Support

[9] WMF-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 Std 802.16-2004, IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed Broadband Wireless Access Systems

[11] IEEE Std 802.16e-2005, IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands

[12] IEEE Std 802.16g-2007, IEEE Standard for Local and metropolitan area networks – Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems – Amendment 3: Management Plane Procedures and Services

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

[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 1034, DOMAIN NAMES - CONCEPTS AND FACILITIES

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

[25] RFC 2131, Dynamic Host Configuration Protocol

[26] RFC 2132, DHCP Options and BOOTP Vendor Extensions

[27] RFC 2461, Neighbor Discovery for IP Version 6 (IPv6)

[28] RFC 2462, IPv6 Stateless Address Autoconfiguration

[29] RFC 2473, Generic Packet Tunneling in IPv6

[30] RFC 2474, Definition of the Differentiated Services Field (DS Field) in the Ipv4 and Ipv6 Headers

[31] RFC 2475, An Architecture for Differentiated Services

[32] RFC 2494, Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type

[33] RFC 2548, Microsoft Vendor-specific RADIUS Attributes

[34] RFC 2560, X.509 Internet Public Key Infrastructure, Online Certificate Status Protocol - OCSP

[35] RFC 2597, Assured Forwarding PHB Group

[36] RFC 2780, IANA Allocation Guidelines For Values In the Internet Protocol and Related Headers

[37] RFC 2784, Generic Routing Encapsulation (GRE)

[38] RFC 2865, Remote Authentication Dial In User Service (RADIUS)

[39] RFC 2866, RADIUS Accounting

[40] RFC 2868, RADIUS Attributes for Tunnel Protocol Support

[41] RFC 2869, RADIUS Extensions

[42] RFC 2890, Key and Sequence Number Extensions to GRE

[43] RFC 3012, Mobile IPv4 Challenge/Response Extensions

[44] RFC 3041, Privacy Extensions for Stateless Address Autoconfiguration in Ipv6

[45] RFC 3046, DHCP Relay Agent Information Option

[46] RFC 3162, RADIUS and IPv6

[47] RFC 3246, An Expedited Forwarding PHB (Per-Hop Behavior)

[48] RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

[49] RFC 3344, IP Mobility Support for IPv4

[50] RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture

[51] RFC 3543, Registration Revocation in Mobile Ipv4

[52] RFC 3576, Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

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

[54] RFC 3587, IPv6 Global Unicast Address Format

[55] RFC 3588, Diameter Base Protocol

[56] RFC 3736, Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6

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

[58] RFC 3775, Mobility Support in IPv6

[59] RFC 3879, Deprecating Site Local Addresses

[60] RFC 3957, Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4, C. Perkins and P. Calhoun, March 2005, Standards Track

[61] RFC 3993, Subscriber-ID Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option

[62] RFC 4004, Diameter Mobile IPv4 Application

[63] RFC 4005, Diameter Network Access Server Application

[64] RFC 4006, Diameter Credit-Control Application

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

[66] RFC 4030, The Authentication Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option

[67] RFC 4072, Diameter Extensible Authentication Protocol (EAP) Application

[68] RFC 4193, Unique Local IPv6 Unicast Addresses

[69] RFC 4282, The Network Access Identifier

[70] RFC 4283, Mobile Node Identifier Option for Mobile IPv6 (MIPv6)

[71] RFC 4284, Identity Selection Hints for the Extensible Authentication Protocol (EAP)

[72] RFC 4285, Authentication Protocol for Mobile IPv6

[73] RFC 4291, IP Version 6 Addressing Architecture

[74] RFC 4366, Transport Layer Security (TLS) Extensions

[75] RFC 4372, Chargeable User Identity

[76] RFC 4541, Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

[77] RFC 4595, Use of IKEv2 in the Fibre Channel Security Association Management Protocol

[78] RFC 4849, RADIUS Filter Rule Attribute

[79] RFC 4862, IPv6 Stateless Address Autoconfiguration

[80] RFC 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments

[81] RFC 5121, Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks

[82] RFC 5213, Proxy Mobile IPv6

[83] RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines

[84] RFC 5692, Transmission of IP over Ethernet over IEEE 802.16 Networks

[85] Draft-ietf-dime-mip6-split-12.txt

[86] RFC 5777, Traffic Classification and Quality of Service (QoS) Attributes for Diameter

[87] draft-ietf-eap-netsel-problem-05.txt

[88] draft-ietf-mip4-gen-ext-01.txt

[89] draft-ietf-mip6-hiopt-12.txt

[90] draft-ietf-pppext-eap-ttls-05.txt

[91] draft-ietf-radext-ieee802-00.txt

[92] draft-yegani-gre-key-extension-03.txt (within a week)

[93] draft-leung-mip4-proxy-mode-08.txt

[94] Internet-Draft “IPv4 Support for Proxy Mobile IPv6” (draft-ietf-netlmm-pmip6-ipv4-support-09)

[95] Internet-Draft “GRE Key Option for Proxy Mobile IPv6” (draft-ietf-netlmm-grekey-option-06)

[96] Internet-Draft “Binding Revocation for IPv6 Mobility” (draft-ietf-mext-binding-revocation-03)

[97] draft-ietf-geopriv-radius-lo-23.txt

[98] Internet-Draft “Prepaid Extensions to Remote Authentication Dial-In User Service (RADIUS)“ draft-lior-radius-prepaid-extensions-16

[99] 3GPP TS29.212 “Policy and Charging Control over Gx reference point”, Release 7

[100] 3GPP TS 32.299 “Charging management; Diameter charging applications”, Release 7

[101] 3GPP TS 32.240 “Charging architecture and principles”, Release 7

[102] IETF RFC 4412, Communications Resource Priority for the Session Initiation Protocol (SIP), Feb. 2006.

[103] 3GPP TS 29.214, Policy and Charging Control over Rx Reference Point, Release 7.

[104] IETF RFC 5127, Aggregation of Diffserv Service Classes, Feb. 2008.

[105] IEEE Std 802.16m™-2011, IEEE Standard for Local and metropolitan area networks - Part 16: Air Interface for Broadband Wireless Access Systems - Amendment 3: Advanced Air Interface.

[106] WMF-T33-001-R016v01, WiMAX Forum Network Architecture, Detailed Protocols and Procedures, Policy and Charging Control, Release 1.6, 11/2010.

[107] 3GPP TS 29.212 “Policy and Charging Control over Gx reference point”, Release 9.2.0, 3/2010.

[108] WMF-T33-109-R016v01, WiMAX Forum Network Architecture, Detailed Protocols and Procedures, Policy and Charging Control, Release 1.6, 11/2010.

[109] 3GPP TS 29.214 “Policy and Charging Control over Rx reference point”, Release 10.3.0, 6/2011.

[110] 3GPP TS 29.214 “Policy and Charging Control over Rx reference point”, Release 9 3.0, 3/2010.

[111] 3GPP TS 29.213 “Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping, Release 9.6.0, 3/2010.

[112] 3GPP TS 29.213 “Policy and Charging Control signalling flows and Quality of Service (QoS) parameter mapping, Release 10.2.0, 6/2011.

[113] WMF-T32-001-R016v01, WiMAX Forum Network Architecture, Architecture Tenets, Reference Model and Reference Points, Base Specification, Release 1.6, 11/2010.

[114] 3GPP TS 23.203 “Policy and Charging Control Architecture”, Release 9, 3/2009.

[115] WMF-T33-115-R015v01, Universal Services Interface, An Architecture for Internet+ Service Model, Nov. 2009.

[116] DRAFT-T33-121-R020v01-A, Architecture, Detailed Protocols and Procedures, WiMAX VoIP Service (WVS), May 2011.

[117] 3GPP TS 24.229, Internet Protocol (IP) Multimedia Call Control Protocol Based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), Stage 3, Release 7, Dec. 2007.

[118] WiMAX Forum, WMF-T33-101-R2001, IMS Interworking, July 20011.

[119] WiMAX Forum, WiMAX – 3GPP EPS Interworking, Phase 2, 2011.

[120] ATIS-1000023.2008, ETS Network Element Requirements for a NGN IMS based Deployments.

[121] WMF-T32-106-WiMAX LI Overview

3. Commonalities of the ASN Control Protocol

This section is applicable to the common protocol on ASN reference points R4, R6 and R8, called the ASN control protocol. In this section:

- the format for the message primitives of the ASN control protocol is defined;
- the transport protocol for the ASN control protocol is defined;
- transport requirements for the ASN control protocol are defined;
- the error handling for the ASN control protocol is defined.

3.1 Encoding and Decoding

Unless otherwise indicated, most significant octets and most significant bits are transmitted first for all data types.

Unless otherwise indicated, Bit #0 of a bit-field is the LSB of the least significant octet and is shown as the rightmost bit. The same rule also applies to bit map and bitmask.

The figure below shows a 32bit bit-field as an example where only Bit#0 is set.

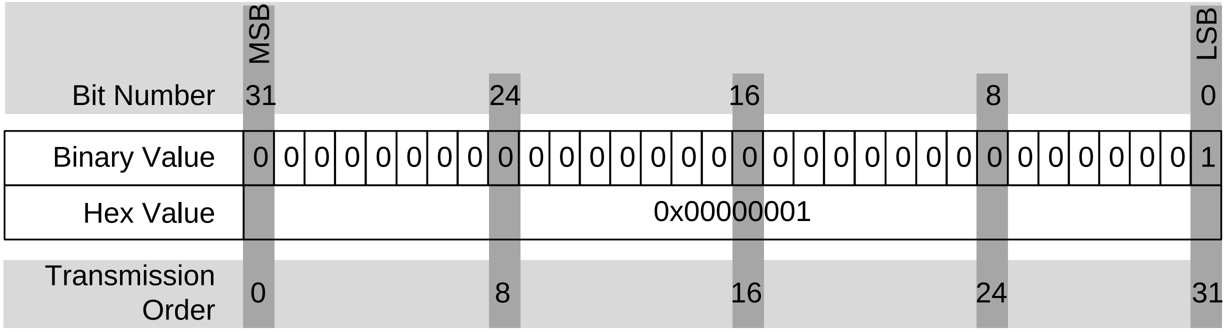


Figure 3-1 – Bit Ordering

3.2 Message Header and Body

The message header starts immediately after the UDP transport header and is followed by message body. Message format (illustrated for IPv4 addresses) for Release 1.x and Release 2.0 is as follows:

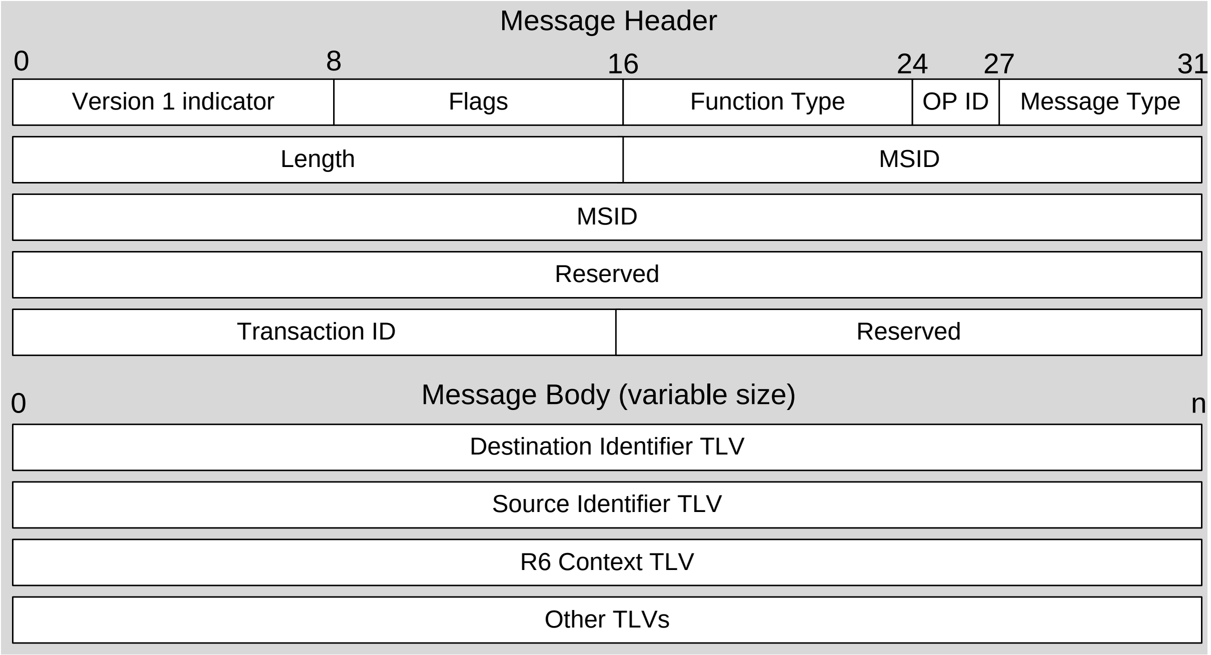


Figure 3-2 – Release 1.x Message Format

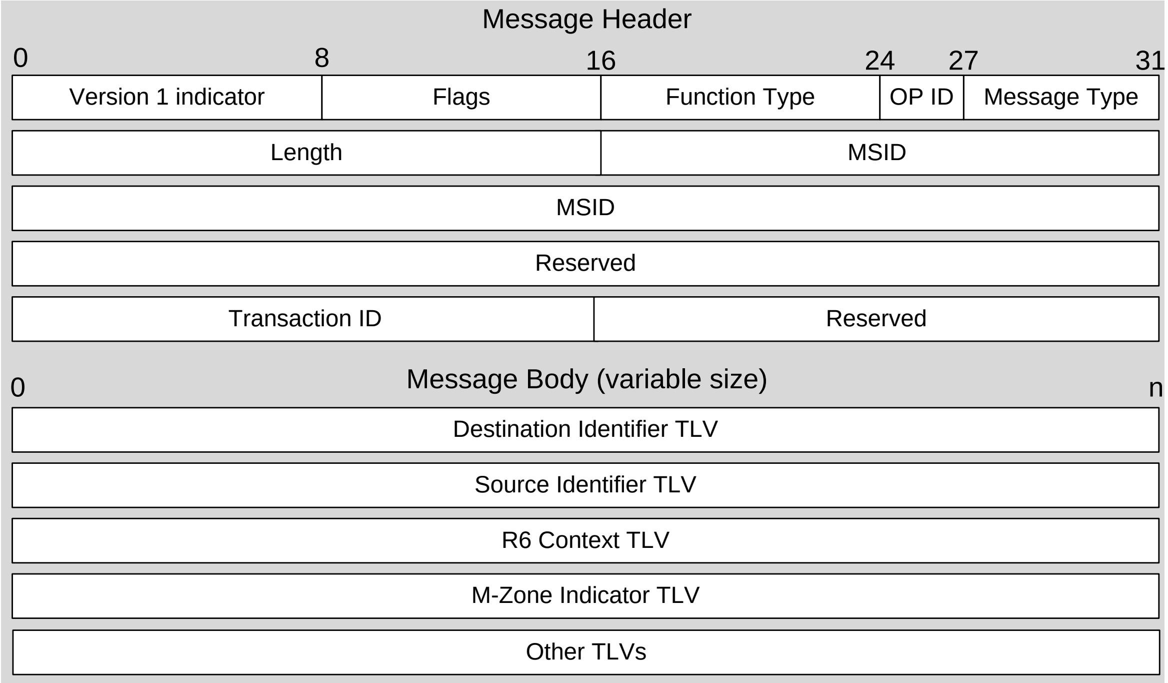


Figure 3-3 – Release 2.0 Message Format

All the fields in the message header are mandatory. The bit ordering depicted in the figure refers to network transmit bit order. All the fields between Release 1.x and Release 2.0 message format are same except adding the M-Zone Indicator TLV in Release 2.0 message format.

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.

r	r	P	E	C	S	T	R

Figure 3-4 – 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 3-5.

– 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.

– P: If this bit is set to”1”, the MSID header field does NOT include the MAC address. When set to “1”, all the bits of the MSID field are set to “0”.

– 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: When the P flag bit is set to "0", the MSID is set to the 6-byte MAC address of MS. For transactions not related to any specific MS, all the bits SHALL be set to zero. If the P flag bit is set to "1", all the bits of the MSID field are set to "0".
- 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:

  - o 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.
  - o 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.

  - o 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 $T_{missing}$ 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 $T_{missing}$ 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.

- M-Zone Indicator TLV: This TLV indicates whether the AMS operates in M-Zone. ABS and Release 2 ASN-GW include this TLV in every message associated with the AMS operating in the M-Zone. The receiver of the message SHALL check whether the M-Zone Indicator TLV is present. If the receiver of the message does not understand this TLV (e.g. legacy ASN-GW), it ignores it.

- 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 3-5 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.

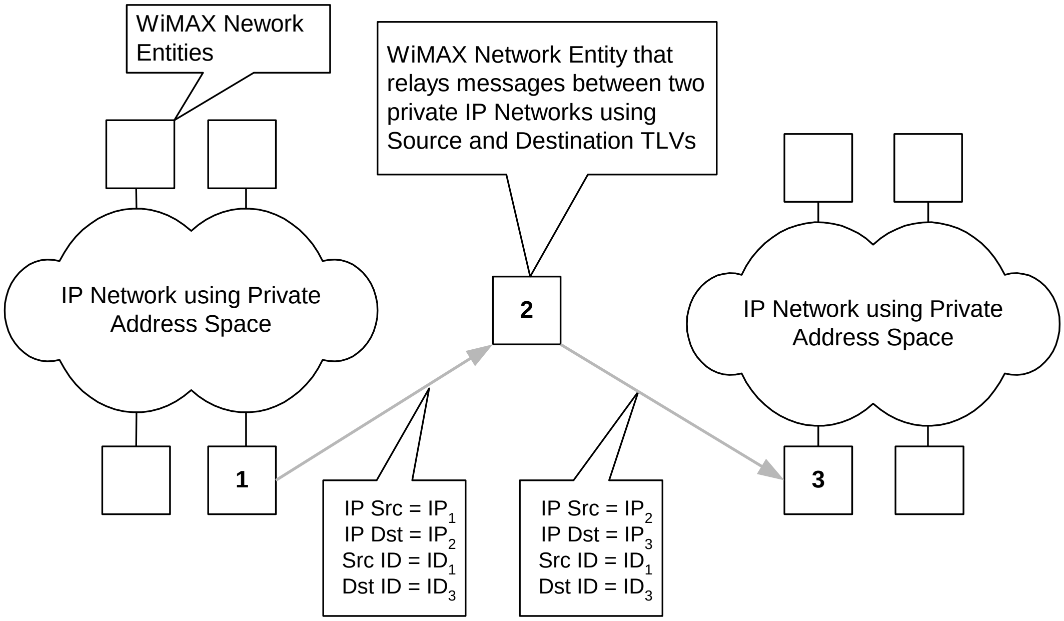

WiMAX Nework Entities
WiMAX Network Entity that relays messages between two private IP Networks using Source and Destination TLVs
IP Network using Private Address Space
2
IP Network using Private Address Space
1
3
IP Src = IP_1
IP Dst = IP_2
Src ID = ID_1
Dst ID = ID_3
IP Src = IP_2
IP Dst = IP_3
Src ID = ID_1
Dst ID = ID_3

Figure 3-5 – 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 3-5, 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 3-6 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.

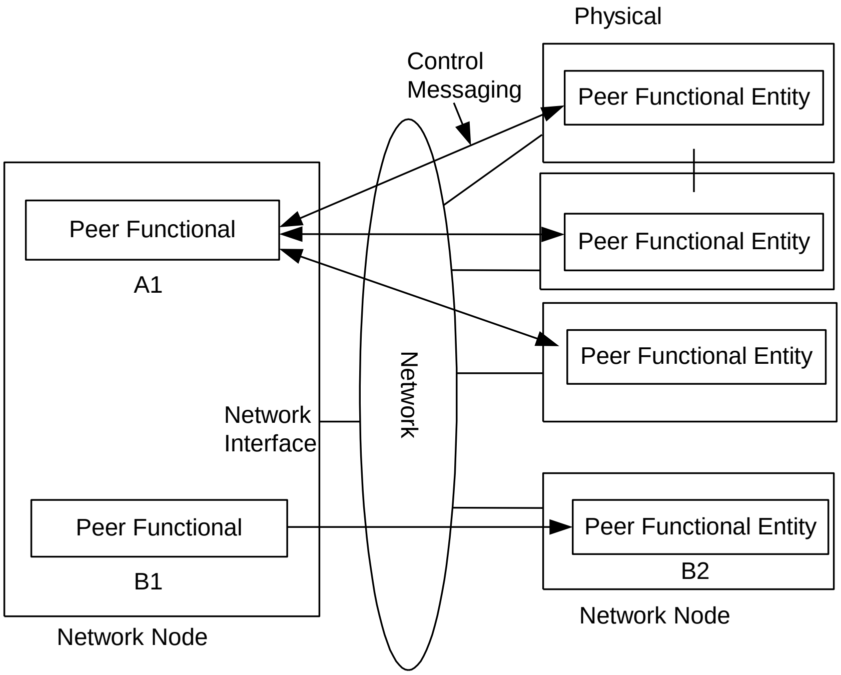


Figure 3-6 – Communication Model

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 Forum® Network Architecture 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 3-7. 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.

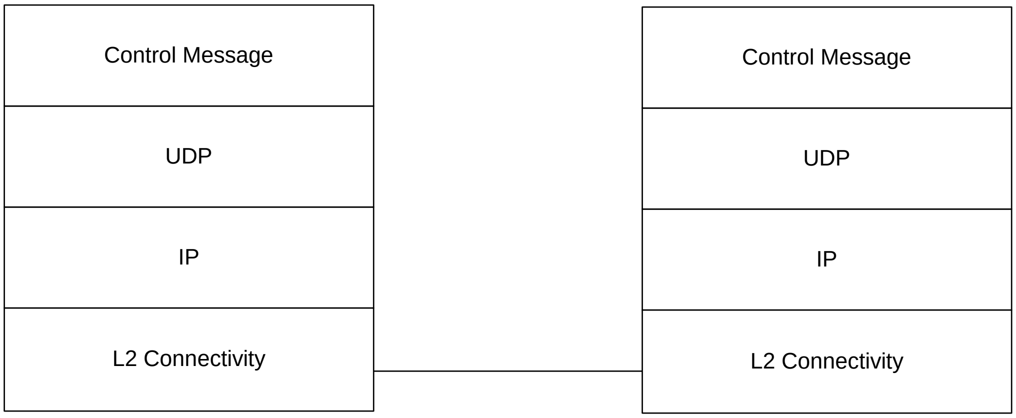


Figure 3-7 – Protocol Layers

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 *Type* value; more TLV with the indicated *Type* value are present in the message resp. TLV than specified in the message definition resp. TLV definition.	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 comprehension is required, the receiver SHALL o diagnose error 'General Message Body Failure' error with attribute ''TLV unexpected'; o and proceed as specified in section 3.5.1.3; o the position of the error is the

		position of the first further occurrence of the TLV in the message requiring comprehension; - otherwise the receiver SHALL skip the remaining occurrences of the TLV.
TLV parsing error	e.g.: - the message is too short to contain the Length field of the TLV; - the message is too short to contain a TLV with indicated length; - or, the TLV is too short to contain all required fields.	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 $T_{missing}$ 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:
  - 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;
  - 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.

If the Source and Destination TLVs and M-Zone Indicator TLV are present, the Failure Indication TLV should be the first TLV included after these TLVs.

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

A. In general, the peer may retransmit the earlier R6/R4 message.

B. The peer can abort the current transaction and may start a new independent transaction. This new transaction may or may not be network exit procedures.

C. The peer can proceed to run network exit procedures.

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

A. If an ‘old’ Acknowledgement message is received in the case of a 3-way transaction, it can be ignored.

B. Last message in every 2-way (e.g., Response) and 3-way transaction (e.g., Acknowledgement) should be kept to accommodate the loss of this last message. If the peer retransmits the previous message, the saved last message should be re-sent without any modification in its original content.

C. In all other cases, the out of order message should be discarded.

3.5.4 Asynchronous Error Indication to Peers

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

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

3.6 MSID Privacy Support in MZone

If MSID Privacy is enabled in the AMS’s home NSP’s policy, the ABS is not aware of the AMS’s real MSID when it enters or re-enters the ASN. ASN entry or re-entry can be done through one of the following procedures:

1. Initial Network Entry
2. Idle Mode Exit – exit from idle mode
3. Location Update during idle mode
4. Uncontrolled Handover

In order for the message recipients to identify the AMS, the message must contain the AMS related information. The following table describes the messages and the related information for each of the mentioned scenario that enables the recipient to find out the AMS’s proper context.

Table 3-3 – Recipient of AMS’s proper context

Scenario (Procedure)	The message	Sender of the message	Receiver of the message	Required information included in the message body (instead of MSID in the header)	Note
Initial Network Entry	MS_PreAttachment_Req	ABS	ASN-GW	MSID*	
	MS_PreAttachment_Rsp	ASN-GW	ABS		
	MS_PreAttachment_Ack	ABS	ASN-GW		

	AR_EAP_Transfer	ABS	ASN-GW		
	AR_EAP-Transfer	ASN-GW	ABS		
	Key_Change_Directive	ASN-GW	ABS		
	Key_Change_Ack	ABS	ASN-GW		
	MS_Attachment_Req	ABS	ASN-GW		
	MS_Attachment_Rsp	ASN-GW	ABS		
	MS_Attachment_Ack	ABS	ASN-GW		
Idle Exit (Re-entry from idle mode)	IM_Exit_StateChange_Req	ABS	ASN-GW	PGID and DID	
	IM_Exit_StageChange_Rsp	ASN-GW	ABS	PGID and DID	Note 2
	IM_Exit_StateChange_Ack	ABS	ASN-GW	PGID and DID	
Location Update	LU-Req	ABS	ASN-GW	PGID and DID	
	LU-Rsp	ASN-GW	ABS	PGID and DID	
	LU-Cnf	ABS	ASN-GW	PGID and DID	
Uncontrolled Handover	Context-Req	T-ABS	S-ABS	Serving BSID and STID	
	Context-Rpt	S-ABS	T-ABS	Serving BSID and STID	Note 2
Note 1. The P bit of flags for all messages indicated above must be set to 1 but MSID* is not used for AMS identification , all the messages shall contain R6 Context ID TLV to distinguish message transactions regarding each AMS. Note 2. IM_Exit_StateChange_Rsp and Context Rpt messages, if MSID is available, must contain the MSID in the message body					

The above indicated messages exchanged during the scenarios SHALL include the required information instead of MSID so that the recipient is able to identify the proper AMS's context. The P bit of flags field of the above indicated messages SHALL be set to 1 so that the receiver is able to notice that the value of MSID field in the header is not the real MSID.

For the message exchanges above which don't include the real MSID value in the header, either party of the communication peers, who is aware of the real MSID, SHALL send it to the other via the indicated messages below. In this way the two peers can use the real MSID. The following messages SHALL contain the MSID in the message body, if an MSID is available, during the indicated message exchange:

1. IM_Exit_StageChange_Rsp during the IM Exit Procedure.

2. Context_Rpt during Uncontrolled Handover from T-ABS to S-ABS.

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 WiMAX Forum® Network Architecture 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/AMS 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.

In order to discover NAP and NSP information a device must scan channels. An MS/AMS may be configured with one or more NSP specific channel plans during manufacture or by an NSP via OTA. An MS/AMS SHALL scan at least all the bands that are specified in the Global Channel Plan [105].

Scanning order

1. Scan most recently connected channel.
2. Scan any stored information like neighbor advertisement information
3. Scan any NSP specific channel plans provisioned if present.
4. Scan all the global channel plans.
5. The device may scan additional channels.

Scanning may be interrupted at any time by automatic selection or user selection of an NSP.

4.1.2 Discovery Procedures

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

4.1.2.1 NAP Discovery

In previous releases (1.*) an MS detects available NAP(s) by scanning and decoding DL-MAP of ASN(s) on detected channel(s). In Release 2.0, an AMS detects available NAP(s) by scanning and decoding P-SFH and S-SFH 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.

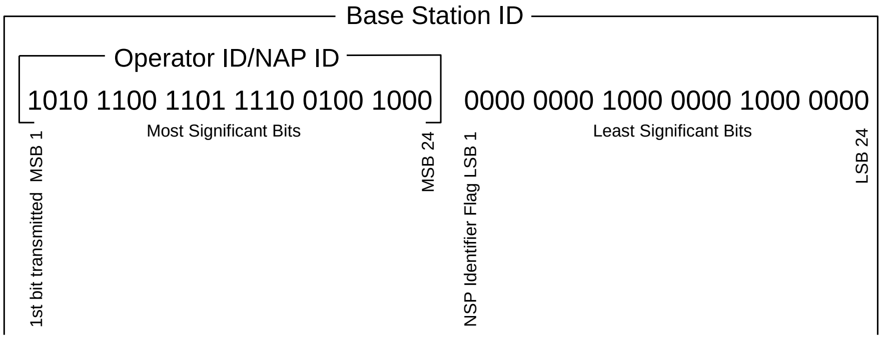


Figure 4-1 – Base Station ID Format for Network Discovery and Selection

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 are managed by IEEE Registration authority[1] which defines the range for global IDs assigned by IEEE and the range for MCC/MNC IDs which can be also used. The field formatting is defined in IEEE Std 802.16. If information useful in MS/AMS 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 4.1.5 for further information).

4.1.2.2 NSP Discovery

4.1.2.2.1 Discovering NSPs Supported by Discovered NAPs

NAPs MAY support one or more NSPs. After the MS/AMS has discovered a NAP (or more than one NAP), it needs to discover the NSP(s) that is (are) supported by the discovered NAP(s). There are several ways for discovering the NSP(s):

1. NSP advertisement by the NAP
2. Over the air information provided by NSP(S) via OTA
3. Pre-configured information during MS/AMS manufacturing

4.1.2.2.1.1 NSP Advertisement by the NAP

Networks that require NSP identifier distinction SHALL signal to the MS/AMS 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/AMS to make a network selection decision. 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 both

[1] IEEE operator ID allocation tutorial: https://standards.ieee.org/regauth/BOPID/Broadband_OperatorID_Tutorial.html

NAP sharing and non-NAP sharing, The BS/ABS SHALL include the change count TLV (the BS includes it in the DCD and the ABS in the S-SFH).

The list of NSP IDs and verbose NSP names are presented over the air interface as part of SII-ADV and/or SBC-RSP (or AAI-SII-ADV and/or AAI-SBC-RSP in advanced air interface) and all NSP realms that can be obtained using SBC-REQ/RSP (or AAI-SBC-REQ/RSP in advanced air interface) SHALL be uniform across all legacy and advanced Base Stations of the same NAP. Also, the NSP change count SHALL be uniform across all legacy and advanced Base Stations of the same NAP. 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’.

Some legacy BSs have the NSP Identifier flag set to 0. Although this is deprecated, the MS/AMS SHALL interpret this as NSP-ID equal to the NAP-ID.

NSP ID is formatted as a 24 bit field that follows the format shown in the following table:

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

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

When using the IEEE-assignable OID for NSP ID format, the OID value SHALL be allocated and administered by the IEEE Registration Authority (RAC)[2]. 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

[2] 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.

Recommendation E.212[3], and mapped to the number space as defined by the IEEE Registration Authority. It is recommended to register the mapped number in the IEEE Registration authority to ensure the coherency and uniqueness of the Operator ID.

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

4.1.2.2.1.2 Over the air information provided by NSP(S)

After establishing a connection with an NSP, the NSP MAY provision the MS/AMS with various information that improves the MS/AMS's ability to discover that NSP. This is performed by provisioning CAPL and RAPL lists; CAPL which define the preferred NAPs to be used for detecting the NSP and the RAPL that lists the preferred visited NSPs to be used when roaming. Note that this information is NSP-specific and the MS/AMS MAY be configured by different NSPs each providing its CAPL and RAPL.

Section 4.1.5 below contains more information on configuration over the air.

4.1.2.2.1.3 Pre-configured information during MS/AMS manufacturing

MS/AMS vendors MAY pre-configure MSs/AMSs during manufacturing with NSP-IDs and their supporting NAP-IDs. It is recommended practice to use the OTA format of Operator ID with corresponding CAPL and RAPL entries.

4.1.3 NSP Enumeration and Selection

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

The MS/AMS SHALL produce a list of available NSPs as discovered through NSP Discovery in the available NAPs, as identified in 4.1.2. The MS/AMS SHALL NOT allow selection of an NSP that has been barred through the forbidden list.

The signal quality is not always used alone as the determining parameter for NSP Selection.

4.1.3.1 Manual Mode

In manual mode the MS/AMS SHALL provide the list of detected NSPs to the connection manager application (the application that displays information to the user and accepts the user-selection of the NSP to connect to) including the following attributes for each NSP:

- The NSP ID
- The verbose NSP name (if available)
- An indication as to whether the user has a subscription(activated via OTA) with this NSP (an HNSP) or not
- If a connection can be established only through a visited NSP (roaming), a roaming indication and the vNSP-ID and verbose name.

Different provisioning states influence the MS/AMS process for NSPs detection and presentation to the user: The display order of NSPs is defined in 4.1.3.1.4.

4.1.3.1.1 Unconfigured State

The MS/AMS is in 'Unconfigured State' if it has no pre-configured information for NSP detection and has not been provisioned by any NSP with NSP detection information (CAPL/RAPL).

[3] 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

In this state, the MS/AMS's only way of obtaining NSP information is if the NAP provides it via SII_ADV and/or SBC_REQ/RSP (AAI-SII-ADV and/or AAI-SBC-REQ/RSp in advance air interface) messages. In that case, the MS/AMS SHALL provide the NSP ID and verbose name of all NSPs that were advertised by all the detected NAPs that advertise information. Since the MS/AMS is not configured, it has no way of detecting HNSPs and will not provide subscription indication. The MS/AMS also does not have any RAPL lists and will not provide roaming indication and visited NSP information.

4.1.3.1.2 Pre-configured inactivated state

Unlike the unconfigured state, the MS/AMS in this state has information for NSP detection that was pre-configured. Although it is pre-configured, it is being used out of the box and thus has no subscription information.

In this state, the MS/AMS generates NSP information for the connection manager application according to the following priorities:

First (highest) priority: The MS/AMS SHALL use the information that is advertised by the detected NAP(s) via the SII_ADV and/or SBC_REQ/RSP (AAI-SII-ADV and/or AAI-SBC-REQ/RSp in advance air interface) messages.

Next priority: The MS/AMS SHALL use pre-configured information to identify the NSPs that are supported by the detected NAPs (for any NAP that has pre-configured information in the MS/AMS).

In this state, the MS/AMS SHALL not generate subscription indications or roaming indications.

4.1.3.1.3 Activated state

In the activated state the MS/AMS has indication of one or more HNSPs – NSPs with which the user has a subscription. In addition to that, the MS/AMS MAY be provisioned with information from time to time by NSPs it connects to for various operations including better NSP detection.

As pre-configured information may be associated with specific NSPs and these NSPs MAY provide information over-the-air while the MS/AMS is connected to them, the over-the-air information MAY augment or override pre-configured information if desired by the NSP.

In this state the MS/AMS generates NSP information for the connection manager application according to the following priorities:

First (highest) priority: The MS/AMS SHALL use the information that is advertised by the detected NAP(s) via the SII_ADV and/or SBC_REQ/RSP (AAI-SII-ADV and/or AAI-SBC-REQ/RSp in advance air interface) messages.

Next priority: The MS/AMS SHALL use pre-configured information and information that was provisioned over the air by NSPs to identify the NSPs that are supported by the detected NAPs.

Third priority: When no HNSP has been detected, and RAPL information exists in the MS/AMS, the MS/AMS SHALL present HNSPs that can be connected to, through visited NSP, together with the detected serving visited NSPs. For each HNSP and VNSP, the NSP ID and verbose name SHALL be provided to the connection manager. The MS/AMS SHALL not provide information about visited NSP that are in the RAPL's forbidden list.

The MS/AMS SHALL provide an indication for all detected HNSPs.

The MS/AMS SHALL provide a roaming indication for all HNSPs that may be reached through the detected VNSPs.

When the MS/AMS is provisioned by NSPs with CAPL information, it will adhere to the NAP selection policy specified in the CAPL (see section 4.1.5 for CAPL details and Table 4-2 for NAP selection policy definition).

When the MS/AMS is provisioned by NSPs with RAPL information and is connecting to the HNSP through a visited NSP, the user may select the visited NSP or configure the MS/AMS to follow the V-NSP selection policy (see section 4.1.5 for RAPL details and Table 4-3 for V-NSP selection policy definition).

HNSPs and those visited NSPs through which an HNSP can be reached SHALL be listed first.

4.1.3.1.4 NSP Display Order

If available, each NSP Enumeration List entry SHALL present only the Verbose NSP Name to the user for selection. If more than one NSP is found, the list SHALL be presented in the following order.

Home NSPs will be presented in user prioritized order if specified. In the case that an HNSP has a RAPL the VNSP list will be presented in RAPL priority order. In rare cases the HNSP could be available directly and alternatively via VNSP. In this rare case a user may select the VNSP if the performance is better due to some condition (for example signal strength).

NSPs that are not activated (HNSPs) or associated with and activated (HNSP) via RAPL (VNSPs) will be displayed in user priority order. If there is no user priority they will be presented below the HNSPs and VNSPs or in a different list.

4.1.3.2 Automatic Mode

In automatic mode, the MS/AMS SHALL detect NSPs and connect to the most appropriate one when possible without user intervention. In order to do so, it requires a priorities list of NSPs to select from.

4.1.3.2.1 User Selection

The user may rank NSPs according to her/his desire. If such a ‘User List’ exists, the MS/AMS SHALL follow this list when selecting the NSP to connect to. The implementation of the ‘User List’ is out of the scope of this specification.

Note that the ‘User List’ may have NSPs which are not activated (i.e. HNSP) in a higher priority and that will cause the MS/AMS to ‘prefer’ a non-activated NSP to an activated NSP while in automatic mode.

The MS/AMS SHALL attempt to select an NSP from the user list according to the order of priority defined in that list. When the NSP is serviced by more than one detected NAP, the MS/AMS selects the NAP that is most appropriate, depending on its provisioned state for that NSP.

4.1.3.2.1.1 Unconfigured State

Since there is no information in the MS/AMS to aid the transformation for detected NAPs to NSPs, the MS/AMS can only (and SHALL) use NSP information that is advertised by the detected NAPs (if supported). If the search for NSPs (from the user list), yields an NSP in the list the MS/AMS SHALL select it. In this state, there are no criteria for selecting the desired NAP (if more than one NAP is serving the searched NSP is reachable).

If none of the NSPs in the user list are detected, the MS/AMS SHALL move to Manual mode.

4.1.3.2.1.2 Pre-configured inactivated state

The MS/AMS SHALL use both advertised information (if supported by the NAP) and pre-configured information to detect NSPs. If there is a contradiction between pre-configured information and the advertised information, the advertised information SHALL be preferred.

If none of the NSPs in the user list are detected, the MS/AMS SHALL move to Manual mode.

4.1.3.2.1.3 Activated state

In activated state, the NSP MAY provide NAP selection criteria (including a forbidden list) to the MS/AMS via CAPL information. The MS/AMS SHALL adhere to CAPL directives (see section 4.1.5-Configuration Information for CAPL details and Table 4-2 for NAP selection policy definition).

If the CAPL’s Selection Policy is not ‘Strict Policy’, the MS/AMS MAY use information that is not in the CAPL as well as the information in the CAPL.

If none of the NSPs in the user list were detected and the MS/AMS has a ‘User Roaming List’ as well as the ‘User List’, the MS/AMS SHALL attempt to roam to one of the NSPs in the user Roaming list (according to the priority specified in that list).

When attempting to roam to the HNSP, the MS/AMS SHALL adhere to the RAPL information to select the V-NSP if provisioned by that HNSP. If the RAPL's Selection Policy is not 'Strict Policy', the MS/AMS MAY attempt to connect to the HNSP via a detected NSP even if it does not appear in the targeted NSP's RAPL or if the RAPL does not exist (this is referred to as 'Opportunistic V-NSP Selection').

If no NSP was detected and no roaming opportunity detected (or if no 'Roaming User List' exists), the MS/AMS SHALL move to Manual mode.

4.1.3.2.2 MS/AMS Selection

If no 'User Selection' list is configured and the MS/AMS is configured to Automatic mode, the MS/AMS selects the NSP and NAP according to its provisioned state.

4.1.3.2.2.1 Unconfigured State

In 'Unconfigured State' the MS/AMS automatically selects an NSP only if it detects a single NSP.

If no NSP was detected or more than one NSP was detected, the MS/AMS SHALL move to Manual mode.

4.1.3.2.2.2 Pre-configured inactivated state

The MS/AMS SHALL use both advertised information (if supported by the NAP) and pre-configured information to detect NSPs and will automatically select an NSP only if it is the single NSP that was detected.

If no NSP was detected or more than one NSP was detected, the MS/AMS SHALL move to Manual mode.

4.1.3.2.2.3 Activated state

In activated state the MS/AMS MAY select the NSP to which it was connected in the previous session, if this mode is supported by the MS/AMS (and enabled by the user).

If only one HNSP is activated (and the MS/AMS is aware of the activation state through OTA indication) or only one HNSP is detected, the MS/AMS SHALL attempt to select that HNSP. If the MS/AMS cannot detect the HNSP (not in range) and configured to 'Automatic Roaming' it SHALL use the RAPL to detect a suitable V-NSP and select it for roaming.

If the MS/AMS is aware of being activated to more than one HNSP and 'connection to last connected HNSP' is not supported, the MS/AMS SHALL move to Manual mode.

4.1.4 ASN Attachment

Following a decision to select an NSP, an MS/AMS 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/AMS. When the NSP Identifier Flag is set to a value of "1", i.e., NAP-Sharing, the MS/AMS SHALL use its NAI with additional information when presented (also known as decorated NAI described in IETF [69]) 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/AMS MAY NOT decorate the realm portion of NAI with the visited NSP realm. The MS/AMS 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/AMS and the identifiers of supported NSPs received from networks are in the list, then these identifiers are mapped locally.

If the MS/AMS does not have the realm of a visited NSP stored in the configuration information such that the MS/AMS 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/AMS MAY include the Visited NSP ID TLV in the SBC-REQ (AAI-SBC-REQ in advanced air interface) message to solicit BS/ABS transmittal of the Visited NSP Realm TLV in the SBC-RSP (AAI-SBC-RSP in advanced air interface) 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 [69]. If the ND&S aware MS/AMS attaches to a non ND&S compliant network and has no preconfigured information about the NAP and NSP, the MS/AMS should attach using EAP TLS with a realm-less NAI, for example - "{sm=1} AABBCCDDEEFF". If the network receives a realm-less NAI, the NAS SHALL route the EAP identity response to the default AAA.

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.

4.1.5 Configuration Information

This sub section describes the content and function of configuration information, which is stored in MS/AMS and used by MS/AMS to assist network entry discovery and selection. Detailed file format of configuration in MS/AMS 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/AMS 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 RALP 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/AMS is not allowed to establish connection to the H-NSP.

If the H-NSP wishes to disable Roaming, it will set the RAPL's Selection Policy to 'Strict Policy' and configuring the MS/AMS with an empty RAPL list.

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 C4of [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.

4.1.6 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.

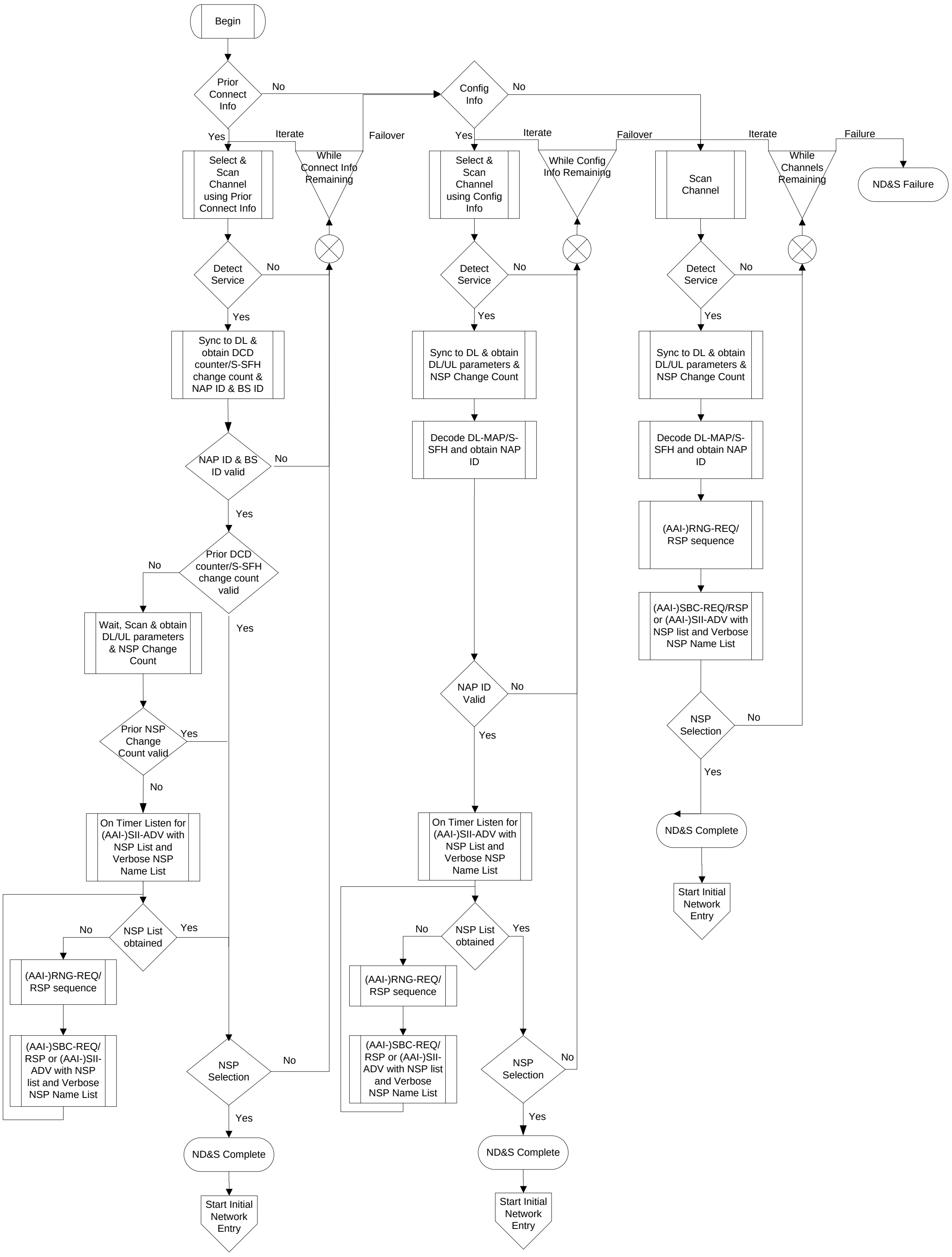

Begin
Prior Connect Info
No
Yes
Iterate
Failover
While Connect Info Remaining
Select & Scan Channel using Prior Connect Info
Detect Service
No
Yes
Sync to DL & obtain DCD counter/S-SFH change count & NAP ID & BS ID
NAP ID & BS ID valid
No
Yes
Prior DCD counter/S-SFH change count valid
No
Yes
Wait, Scan & obtain DL/UL parameters & NSP Change Count
Prior NSP Change Count valid
Yes
No
On Timer Listen for (AAI-)SII-ADV with NSP List and Verbose NSP Name List
NSP List obtained
No
Yes
(AAI-)RNG-REQ/ RSP sequence
(AAI-)SBC-REQ/ RSP or (AAI-)SII-ADV with NSP list and Verbose NSP Name List
NSP Selection
No
Yes
ND&S Complete
Start Initial Network Entry
Config Info
No
Yes
Iterate
Failover
Select & Scan Channel using Config Info
While Config Info Remaining
Detect Service
No
Yes
Sync to DL & obtain DL/UL parameters & NSP Change Count
Decode DL-MAP/S-SFH and obtain NAP ID
NAP ID Valid
No
Yes
On Timer Listen for (AAI-)SII-ADV with NSP List and Verbose NSP Name List
NSP List obtained
No
Yes
(AAI-)RNG-REQ/ RSP sequence
(AAI-)SBC-REQ/ RSP or (AAI-)SII-ADV with NSP list and Verbose NSP Name List
NSP Selection
No
Yes
ND&S Complete
Start Initial Network Entry
Iterate
Failure
Scan Channel
While Channels Remaining
ND&S Failure
Detect Service
No
Yes
Sync to DL & obtain DL/UL parameters & NSP Change Count
Decode DL-MAP/S-SFH and obtain NAP ID
(AAI-)RNG-REQ/ RSP sequence
(AAI-)SBC-REQ/RSP or (AAI-)SII-ADV with NSP list and Verbose NSP Name List
NSP Selection
No
Yes
ND&S Complete
Start Initial Network Entry

Figure 4-2 – Network Discovery and Selection SDL

4.1.6.1 Process Flow Descriptions

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

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

Prior Connect Info: The MS/AMS assesses the presence of stored configuration information (see section 4.1.5).

- if the MS/AMS has stored configuration information of prior legacy or advanced base stations' PHY characteristics, suitable and useful for reducing the channel scanning and synchronization options, then the MS/AMS uses this information to selectively search for those legacy or advanced base stations in 'Select & Scan Channel using Prior Connect Info'.
- else if the MS/AMS does not have prior legacy or advanced base stations' PHY characteristics, the MS/AMS 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/AMS conducts channel selection and detection of available BS/ABS using the stored configuration information.

Detect Service: the MS/AMS attempts to detect a legacy or advanced base station with the expected PHY characteristics on the tested channel.

- if the MS/AMS detects a legacy or advanced base station operating with the expected PHY characteristics on the tested channel, the MS/AMS proceeds to 'Sync to DL & obtain DCD counter (S-SFH change count in advanced air interface) & NAP ID & BS ID'.
- else if the MS/AMS fails to detect a BS/ABS on the channel, and while untested channels based on the stored configuration remain, the MS/AMS repeats the 'Select & Scan Channel using Prior Connect Info' process, iterating to the next channel and BS/ABS for assessment; if no untested channels remain, the MS/AMS proceeds with detection and selection based on 'Config Info'.

Sync to DL & obtain DCD counter (S-SFH change count in advanced air interface) & NAP ID & BS ID': The MS/AMS synchronizes to the DL transmissions and obtains the DCD counter from the DL-MAP (change count from the S-SFH in advanced air interface).

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

- if the MS/AMS determines that the detected NAP ID & BS ID matches the stored, expected values, the MS/AMS continues with 'Prior DCD counter (change count from the S-SFH in advanced air interface) valid '.
- else if the MS/AMS 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/AMS repeats the 'Select & Scan Channel using Prior Connect Info' process, iterating to the next channel and BS/ABS for assessment; if no untested channels remain, the MS/AMS proceeds with detection and selection based on 'Config Info'.

Prior DCD counter (change count in advanced air interface) valid: The MS/AMS assesses the validity of the detected DCD counter (change count in advanced air interface).

- if the MS/AMS determines that the detected DCD counter (change count in advanced air interface) value matches the stored, expected DCD counter (change count in advanced air interface) value, then the MS/AMS continues to 'NSP Selection'.
- else if the MS/AMS determines that the detected DCD counter (change count in advanced air interface) is different than the stored, expected DCD counter (change count in advanced air interface) value, the MS/AMS SHALL 'Wait, Scan & obtain DL/UL parameters & NSP Change Count'.

Wait, Scan & obtain DL/UL parameters & NSP Change Count: For MS/AMS that detect a DCD counter (change count in advanced air interface) different than the stored, expected value, the MS/AMS wait and listen for the transmission of the updated NSP Change Count, if present, and continues with 'Prior NSP Change Count valid'.

Prior NSP Change Count valid: When NSP Change Count is present in DCD/S-SFH, the MS/AMS tests the detected NSP Change Count.

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

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

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

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

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

(AAI-)SBC-REQ; (AAI-)SBC-RSP or (AAI-)SII-ADV with NSP List and Verbose NSP Name List: The MS/AMS conducts (AAI-)SBC-REQ message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS/ABS transmittal of NSP List TLV, either through an (AAI-)SII-ADV broadcast or (AAI-)SBC-RSP unicast transmission, and may include SIQ TLV with bit 1 set to a value of '1' during network entry to solicit BS/ABS 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/AMS conducts automatic NSP selection (see section 4.1.3) or manual NSP selection (see section 4.1.3).

- if the NAP ID and NSP ID detected will connect the MS/AMS to its home CSN for authentication during network entry, and MS/AMS 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/AMS repeats the 'Select & Scan Channel using Prior Connect Info' process, iterating to the next channel and BS/ABS for assessment; if no untested channels remain, the MS/AMS proceeds with detection and selection based on 'Config Info'.

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

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

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

Configuration Info: The MS/AMS assesses the presence of stored configuration information (see section 4.1.5).

- if the MS/AMS has stored configuration information of legacy and advanced 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/AMS uses this information to selectively search for those legacy and advanced base stations in 'Select & Scan Channel using configuration Info'.
- else if the MS/AMS does not have prior legacy and advanced base stations' PHY characteristics by subscription programmed values, the MS/AMS defaults to selection and detection based on the physical scan capabilities of the MS/AMS device through 'Scan Channel'.

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

Detect Service: the MS/AMS attempts to detect a legacy and advanced base station with the expected PHY characteristics on the tested channel.

- if the MS/AMS detects a legacy and advanced base station operating with the expected PHY characteristics on the tested channel, the MS/AMS proceeds to 'Sync to DL & obtain DL/UL parameters & NSP Change Count'.
- else if the MS/AMS fails to detect a BS/ABS on the channel, and while untested channels based on the stored configuration remain, the MS/AMS repeats the 'Select & Scan Channel using configuration Info' process, iterating to the next channel and BS/ABS for assessment; if no untested channels remain, the MS/AMS proceeds with detection and selection based on 'Scan Channel'.

Sync to DL & obtain DL/UL parameters & NSP Change Count: The MS/AMS synchronizes to the DL transmissions and listens for the transmission of the updated DL/UL parameters.

Decode DL-MAP/S-SFH and obtain NAP ID: The MS/AMS listens for and decodes DL-MAP/S-SFH, obtaining the NAP ID.

NAP ID valid: The MS/AMS tests the detected NAP ID.

- if the MS/AMS determines that the detected NAP ID matches the stored, expected values, the MS/AMS continues 'On Timer Listen for (AAI-)SII-ADV message with NSP List and Verbose NSP Name List'.
- else if the MS/AMS determines that the detected NAP ID does not match the stored, expected value, and while untested channels based on the stored configuration remain, the MS/AMS repeats the 'Select & Scan Channel using configuration Info' process, iterating to the next channel and BS/ABS for assessment; if no untested channels remain, the MS/AMS proceeds with detection and selection based on 'Scan Channel'.

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

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

- if the MS/AMS obtained the list of NSP IDs, proceed to 'NSP Selection'.
- else the MS/AMS uses the SBC query process to obtain the NSP List, proceed with '(AAI-)RNG-REQ/RSP sequence'.

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

(AAI-)SBC-REQ; (AAI-)SBC-RSP or (AAI-)SII-ADV with NSP list and Verbose NSP Name List: The MS/AMS conducts (AAI-)SBC-REQ message including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS/ABS transmittal of NSP List TLV, either through an (AAI-)SII-ADV broadcast or (AAI-)SBC-RSP unicast transmission, and may include SIQ TLV with bit 1 set to a value of '1' during network entry to solicit BS/ABS 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/AMS conducts automatic NSP selection (see section 4.1.3) or manual NSP selection (see section 4.1.3).

- if the NAP ID and NSP ID detected will connect the MS/AMS to its home CSN for authentication during network entry, and MS/AMS 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/AMS repeats the 'Select & Scan Channel using configuration Info' process, iterating to the next channel and BS/ABS for assessment; if no untested channels remain, the MS/AMS proceeds with detection and selection based on 'Scan Channel'.

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

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

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

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

Detect Service: the MS/AMS attempts to detect a legacy or advanced base station on the tested channel.

- if the MS/AMS detects a legacy or advanced base station operating on the tested channel, the MS/AMS proceeds to 'Sync to DL & obtain DL/UL parameters & NSP Change Count'.
- else if the MS/AMS fails to detect a BS/ABS on the channel, and while untested channels based on the physical scan capabilities of the MS/AMS device remain, the MS/AMS repeats the 'Scan Channel' process, iterating to the next channel for assessment; if no untested channels remain, the MS/AMS proceeds with 'ND&S failure'.

Sync to DL & obtain DL/UL parameters & NSP Change Count: The MS/AMS synchronizes to the DL transmissions and listens for the transmission of the updated DL/UL parameters.

Decode DL-MAP/S-SFH and obtain NAP ID: The MS/AMS listens for and decodes DL-MAP/S-SFH, obtaining the NAP ID.

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

(AAI-)SBC-REQ; (AAI-)SBC-RSP or (AAI-)SII-ADV with NSP list and Verbose NSP Name List: The MS/AMS conducts (AAI-)SBC-REQ; then MS/AMS transmits (AAI-)SBC-REQ including SIQ TLV with bit 0 set to a value of '1' during network entry to solicit BS/ABS transmittal of NSP List TLV, either through an (AAI-)SII-ADV broadcast or (AAI-)SBC-RSP unicast transmission, and may include SIQ TLV with bit 1 set to a value of '1' during network entry to solicit BS/ABS transmittal of Verbose NSP Name List TLV, to be transmitted along with NSP List TLV proceed with 'NSP Selection'.

NSP Selection: The MS/AMS conducts automatic NSP selection (see section 4.1.3) or manual NSP selection (see section 4.1.3).

- if the NAP ID and NSP ID detected will connect the MS/AMS to its home CSN for authentication during network entry, and MS/AMS decides to do NSP and NAP selection at this point of scanning, the process proceeds to 'ND&S Complete'.
- else while untested channels remain, the MS/AMS repeats the 'Scan Channel' process, iterating to the next channel and BS/ABS for assessment; if no untested channels remain, the MS/AMS proceeds with 'ND&S failure'.

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

ND&S Failure: The MS/AMS failed the network detection and selection procedure. It SHALL either notify the user of the failure or re-attempt an additional ND&S attempt (possible after a certain time delay when energy conservation is required).

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

4.2 IP Addressing

4.2.1 IPv4 Addressing

Functional entities and architecture for IPv4 addressing are described in Stage 2 section 7.2.1. Details on how IPv4 addressing is performed via DHCP, FIAA (Fast IP Address Allocation), PMIP4, PMIP6, and CMIP4 are described in Stage 3 section 4.8. Details on how IPv4 addressing is performed for Simple IP is described in Stage 3 Section 4.13.

4.2.2 IPv6 Addressing

IPv6 addressing details are described in Stage 3 section 4.10.5.9. Addressing principles and restrictions for PMIP6 are described in Stage 2 section 7.2.2.5. Details on how addressing is performed via stateless address autoconfiguration, DHCP (DHCPv4 or DHCPv6), and FIAA are specified in Stage 3 section 4.8.5.

4.3 WiMAX® Key Hierarchy and Distribution

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

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

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

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

The MS/AMS SHALL be authenticated by the HNSP using its subscriber credential. Additionally, the HNSP MAY perform authentication on the device credential as well. See section 4.4.1 for more details.

The MS/AMS and the network perform authentication using EAP ([57]). The EAP method selected SHALL be capable of producing MSK and EMSK.

MSK and EMSK generated from the EAP authentication are used to derive other keys (e.g., PKMv2/PKMv3 and Mobile IP keys).

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

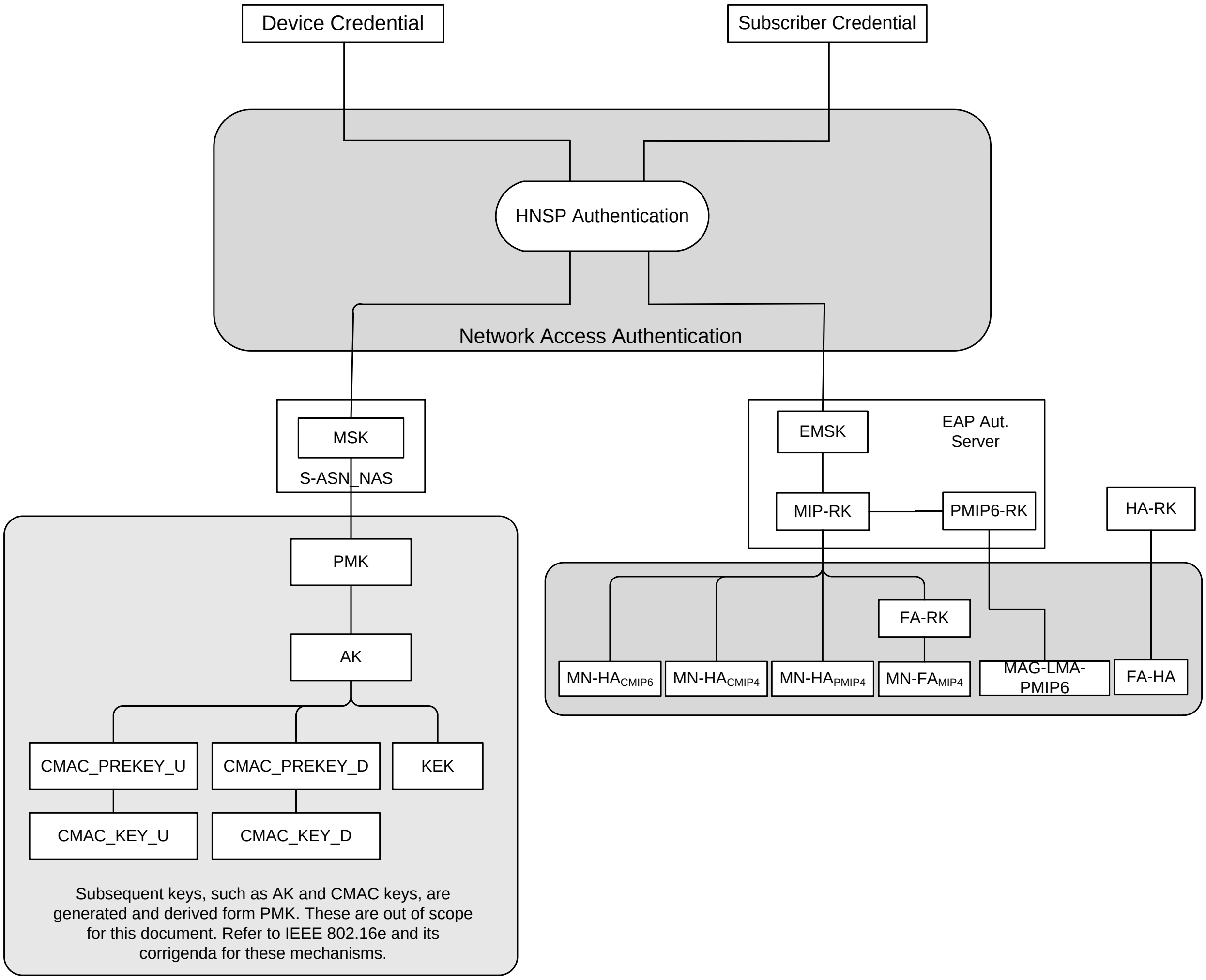
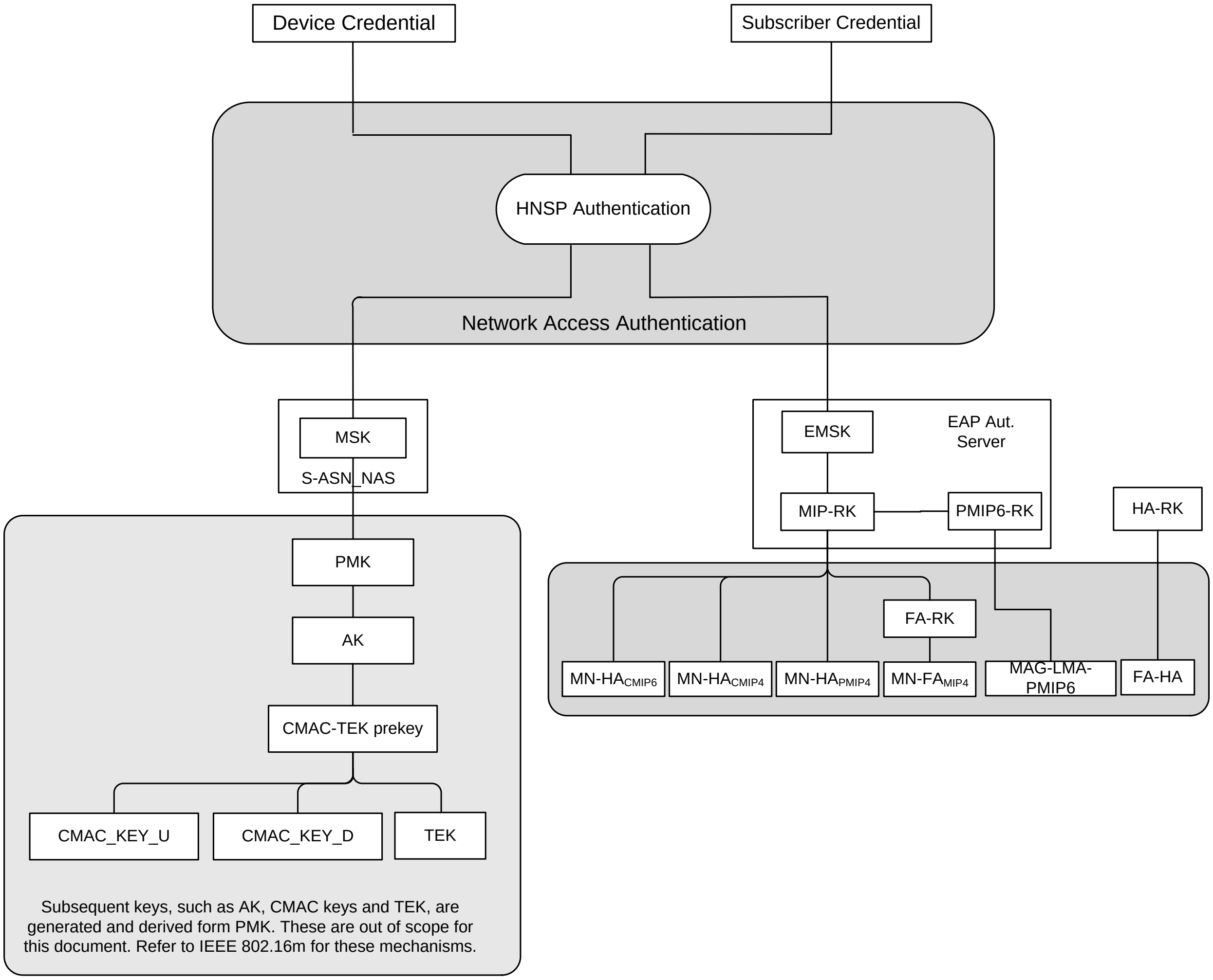


Figure 4-3 – (a) WiMAX® Key Hierarchy supporting PKMv2



Subsequent keys, such as AK, CMAC keys and TEK, are generated and derived form PMK. These are out of scope for this document. Refer to IEEE 802.16m for these mechanisms.

Figure 4-4 – (b) WiMAX® Key Hierarchy supporting PKMv3

The MS/AMS 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/AMS and the BS/ABS (R1) respectively.

The EMSK stays in the EAP layer in the MS/AMS 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/AMS.

4.3.1.1 Key Generation

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

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

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

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

where:

usage-data = key label + “\0” + length

key label = miprk@wimaxforum.org in ASCII

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

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

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

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:

PMIP6-RK-1 = HMAC-SHA256(MIP-RK , usage-data | 0x01)

PMIP6-RK-2 = HMAC-SHA256(MIP-RK, PMIP6-RK-1 | usage data | 0x02)

PMIP6-RK = PMIP6-RK-1 | PMIP6-RK-2

where:

usage-data = key label + “\0” + length

key label = pmip6rk@wimaxforum.org in ASCII

length = 0x0200 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:

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

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

In order to prevent potential collisions between values of SPI generated using this procedure, the process defined in Sec. 4.3.1.1.1 SHALL be used. Once all conditions in Sec. 4.3.1.1.1 are satisfied, e.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 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 4-5.

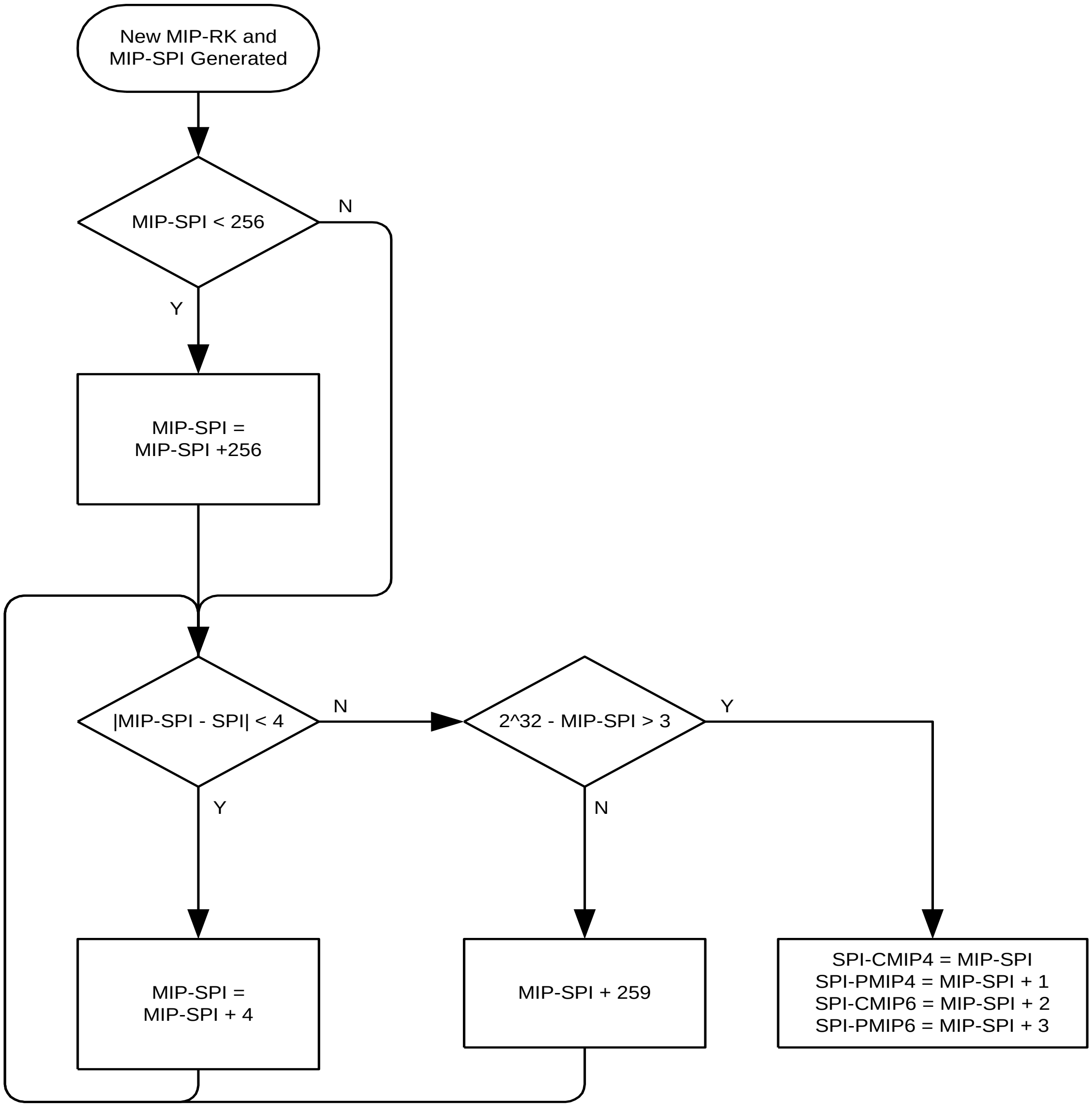


Figure 4-5 – SPI Collision Avoidance Mechanism

4.3.1.2 Key Distribution

As specified above, the MIP-RK key is derived at the MS/AMS 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/AMS 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.

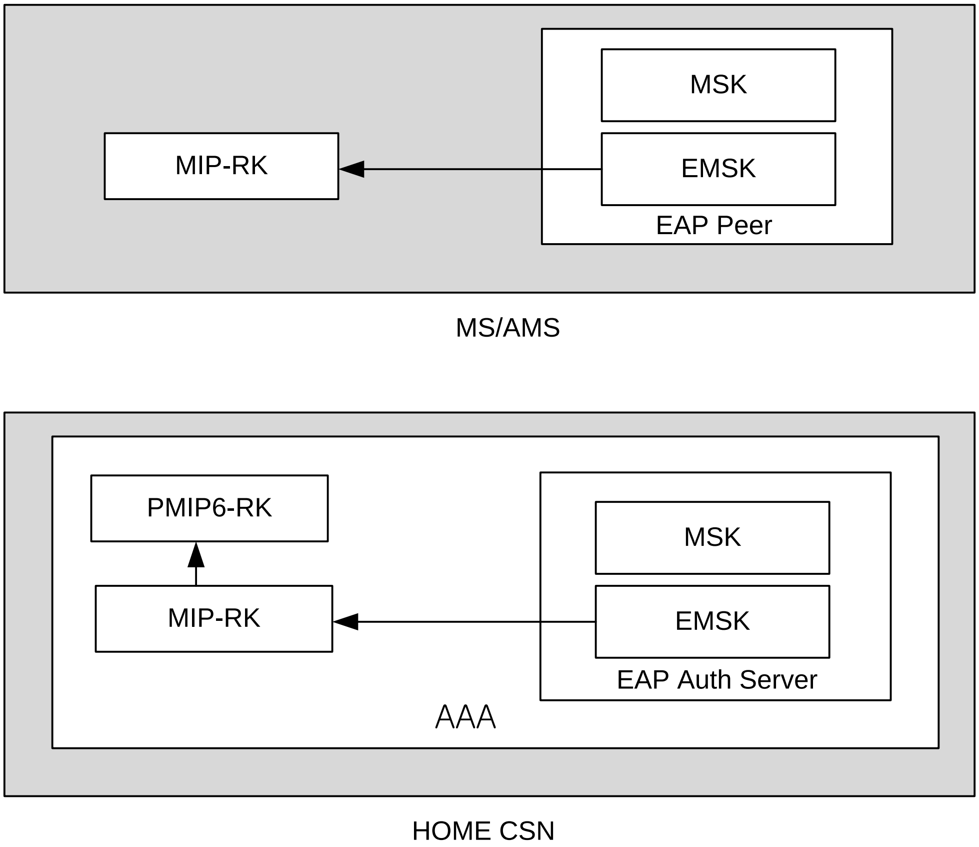


Figure 4-6 – Key Distribution

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.

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

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

4.3.2 AK Key

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

4.3.2.1 Key Generation

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

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

```
PMK = truncate (MSK, 160)
```

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

In case of PKMv2,

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

In case of PKMv3,

```
AK = Dot16KDF (PMK, MS Addressing|BSID|“AK”, 160),
```

where MS Addressing is valued as follows.

If either S-SFH Network Configuration bit = 0b0 when MSID privacy is disabled or S-SFH Network Configuration bit = 0b1, the value of MS Addressing shall be 48bit MS MAC Address. Otherwise, the value of MS Addressing shall be MSID*.

RSA authtentication is not used in WiMAX, hence EIK has been depricated.

4.3.2.2 Key Lifetime

AK lifetime equals the PMK remaining lifetime.

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

AK lifetime is transferred from Authenticator to BS/ABS as part of the AK Context.

After BS/ABS's Resource Retain Timer expires, or BS/ABS receives *HO_Complete* message from backbone network, BS/ABS SHALL remove the AK and its contexts even before its lifetime expires.

In the operations of BS or Lzone of ABS, after BS/ABS(LZone) receives the MOB_HO-IND with HO_IND type =0b00 under the situation that BS/ABS(LZone) handovers using MOB_BSHO-REQ or MOB_BSHO-RSP with Resource Retain Flag set to '0', BS/ABS(LZone) SHALL remove the AK and its contexts even before its lifetime expires also.

4.3.3 AK SN, PMK SN Usage and AK Context

4.3.3.1 Clarification of AK SN and PMK SN

PMK SN is a 4 bit values.

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

4.3.3.2 PMK SN Usage in Initial Authentication

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

4.3.3.3 PMK SN Usage in Re-authentication

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

4.3.3.4 AK SN Derivation from PMK SN

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

AK SN SHALL equal PMK SN.

Note: The AK Context is defined in Table 204 and 765 of 802.16 for PKM v2 and v3 respectively.

4.3.4 CMAC Keys and Replay Protection for Management Messages

The IEEE 802.16defines 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/AK_COUNT. Note that CMAC_KEY_COUNT is named as AK_COUNT in PKMv3 and CMAC_KEY_COUNT is used instead of AK_COUNT if misunderstanding is not expected. Maintenance of this counter by the MS/AMS and network, as well as the simplified process flowchart, are depicted in the following subsections.

For simplicity, in this section the CMAC_KEY_COUNT/AK_COUNT is also denoted as *N*. The value of this count maintained by the MS/AMS is denoted as CMAC_KEY_COUNT$_M$/AK_COUNT$_M$ or *X*, the count value maintained by the BS/ABS is denoted as CMAC_KEY_COUNT$_B$/AK_COUNT$_B$ or *Y*, and the value maintained by the Anchor Authenticator is denoted as CMAC_KEY_COUNT$_N$/AK_COUNT$_N$ or *Z*.

4.3.4.1 Maintenance of CMAC_KEY_COUNT/AK_COUNT by MS/AMS

Upon successful completion of the PKMv2/v3 Authentication or Re-authentication, and establishment of a new PMK, the MS/AMS SHALL reset the CMAC_KEY_COUNT$_M$/AK_COUNT$_M$ (*X*) to zero. In particular, this reset SHALL occur upon reception of the SA-TEK Challenge/Key_Agreement-MSG#1 message. The MS/AMS SHOULD initiate re-authentication when the CMAC_KEY_COUNT$_M$/AK_COUNT$_M$ reaches a value of 32768. Note, that MS/AMS SHALL manage a separate CMAC_KEY_COUNT$_M$/AK_COUNT$_M$ for every active PMK context. Specifically, during reauthentication, after EAP completion, but before the new PMK activation, the old CMAC_KEY_COUNT$_M$/AK_COUNT$_M$ (as per old PMK) is used for CMAC generation of MAC control messages, while the new CMAC_KEY_COUNT$_M$/AK_COUNT$_M$ (which is initialized from zero) is used for CMAC generation for PKMv2 3-way handshake messages/PKMv3 Key_Agreement 3-way handshake messages. The old CMAC_KEY_COUNT$_M$/AK_COUNT$_M$ is deleted together with the old PMK context. The count of zero SHALL be used to generate the CMAC_KEY_* keys that in turn are used to authenticate that message. Also at this time, the counts in the serving BS/ABS and Authenticator SHALL be set to zero and one respectively.

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

The value of AK_COUNT and CMAC_KEY_COUNT are always same and conveyed through the same TLV.

4.3.4.1.1 CMAC_Key_Count_Lock/CMAC_Key_Count_Unlock and AK_COUNT_Lock/AK_COUNT_Unlock States

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

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

4.3.4.2 Maintenance of CMAC_KEY_COUNT/AK_COUNT by the Network

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

4.3.4.2.1 Processing of CMAC_KEY_COUNT/AK_COUNT by the BS/ABS

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

Upon successful completion of the PKMv2/v3 Authentication or Re-authentication, and establishment of a new PMK, the BS/ABS SHALL reset the $CMAC\_KEY\_COUNT_B$/AK_COUNT_B (*Y*) to zero. The BS/ABS 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/Key_Agreement-MSG#1 message. Note, that BS/ABS SHALL manage a separate $CMAC\_KEY\_COUNT_B$/AK_COUNT_B for every active AK context. Specifically, during reauthentication, after EAP completion, but before the new PMK activation, the old $CMAC\_KEY\_COUNT_B$/AK_COUNT_B (as per old PMK/ AK) is used for CMAC generation of MAC control messages, while the new $CMAC\_KEY\_COUNT_B$/AK_COUNT_B (which is initialized from zero) is used for CMAC generation for PKMv2 3-way handshake messages/PKMv3 Key_Agreement 3-way handshake messages. The old $CMAC\_KEY\_COUNT_B$/AK_COUNT_B is deleted together with the old PMK/ AK context. The count of zero SHALL be used to generate the CMAC_KEY_* keys that in turn are used to authenticate that message.

If the BS/ABS does not possess the value of $CMAC\_KEY\_COUNT_B$/AK_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/ABS MAY use the *Context_Req* / *Context_Rpt* transaction for this purpose.

If the BS/ABS obtains the AK Context including the $CMAC\_KEY\_COUNT_N$/AK_COUNT_N (Z) from the Anchor Authenticator, the BS/ABS SHALL set $CMAC\_KEY\_COUNT_B$/AK_COUNT_B = $CMAC\_KEY\_COUNT_N$/AK_COUNT_N (Y = Z).

Upon receiving the RNG-REQ/AAI-RNG-REQ message from the MS/AMS containing the CMAC_KEY_COUNT TLV/AK_COUNT attribute, the BS/ABS SHALL compare the received count value CMAC_KEY_COUNT$_{M}$/AK_COUNT$_{M}$ with the CMAC_KEY_COUNT$_{B}$/AK_COUNT$_{B}$ (*X*<>*Y*).

If CMAC_KEY_COUNT$_{M}$/AK_COUNT$_{M}$ < CMAC_KEY_COUNT$_{B}$/AK_COUNT$_{B}$, and the RNG-REQ/AAI-RNG-REQ message is received as a part of reentry or HO, the BS/ABS SHALL send the RNG-RSP/AAI-RNG-RSP message rejecting an access and indicating that MS/AMS SHALL conduct full re-authentication.

If CMAC_KEY_COUNT$_{M}$/AK_COUNT$_{M}$ ≥ CMAC_KEY_COUNT$_{B}$/AK_COUNT$_{B}$, the BS/ABS SHALL do the following:

The BS/ABS SHALL use the CMAC_KEY_COUNT$_{M}$/AK_COUNT$_{M}$ to compute a temporary value of CMAC_KEY_U$_{T}$, and use the CMAC_KEY_U$_{T}$ to validate the CMAC digest present in the RNG-REQ/AAI-RNG-REQ message.

If the CMAC digest is not valid, and the RNG-REQ/AAI-RNG-REQ message is received as a part of reentry, HO, or Secure Location Update, the BS/ABS SHALL send the RNG-RSP/AAI-RNG-RSP message rejecting an access and indicating that MS/AMS SHALL conduct full re-authentication. In addition, the BS/ABS 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 CMAC_KEY_COUNT$_{M}$/AK_COUNT$_{M}$ = CMAC_KEY_COUNT$_{B}$/AK_COUNT$_{B}$, the BS/ABS SHALL send the RNG–RSP/AAI-RNG-RSP message to the MS/AMS allowing legitimate access. Once an access is completed, the BS/ABS SHALL inform the Anchor Authenticator of the successful access by using the R6 *CMAC_Key_Count_Update* message.
- If CMAC digest is valid, and CMAC_KEY_COUNT$_{M}$/AK_COUNT$_{M}$ > CMAC_KEY_COUNT$_{B}$ /AK_COUNT$_{B}$, the BS/ABS SHALL send the RNG-RSP/AAI-RNG-RSP message to the MS/AMS allowing legitimate access. Once an access is completed, the BS/ABS SHALL inform the Anchor Authenticator of the successful access by using the R6 *CMAC_Key_Count_Update* message and include the CMAC_KEY_COUNT$_{M}$/AK_COUNT$_{M}$ in the message.

4.3.4.2.2 Processing of CMAC_KEY_COUNT/AK_COUNT by the Anchor Authenticator

The Anchor Authenticator SHALL maintain the CMAC_KEY_COUNT$_{N}$/AK_COUNT$_{N}$ for every MS/AMS as part of its security context, called the AK Context, and associated with the PMK. When the Anchor Authenticator for the MS/AMS is relocated, and the associated AK context for the MS/AMS is deleted in the old Anchor Authenticator, the value of CMAC_KEY_COUNT$_{N}$/AK_COUNT$_{N}$ is also deleted.

Upon successful completion of the PKMv2/v3 Authentication or Re-authentication, and creation of a new PMK, the Anchor Authenticator SHALL set the CMAC_KEY_COUNT$_{N}$/AK_COUNT$_{N}$ for the MS/AMS 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/ABS, the Anchor Authenticator SHALL return the current value of the CMAC_KEY_COUNT$_{N}$/AK_COUNT$_{N}$ in the *Context_Rpt* message.

Upon receiving the indication of the successful access from the BS/ABS in the R6 *CMAC_Key_Count_Update* message containing the CMAC_KEY_COUNT$_{M}$/AK_COUNT$_{M}$, the Anchor Authenticator SHALL compare it to the locally maintained value of CMAC_KEY_COUNT$_{N}$/AK_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$_{M}$) and

AK_COUNT$_{N}$ = MAX(AK_COUNT$_{N}$, AK_COUNT$_{M}$)

in other words,

Z = MAX(Z, X)

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

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/AMS and the target BS/ABS, thus no CMAC_KEY_* keys based on the incremented count have been used to generate message digests. Therefore, the CMAC_KEY_COUNT/AK_COUNT counters in the MS/AMS, BS/ABS, 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.

When AMS resuming communications with the serving ABS(MZone), it notifies the incremented current AMS AK_COUNT_M to the ABS using AAI-HO-IND message. The serving ABS SHALL then inform the Anchor Authenticator of this new value by using the R6 *CMAC_Key_Count_Update* message and the Authenticator SHALL re-sync its AK_COUNT_N accordingly, but legacy Authenticator may be not supporting that re-synchronization of AK_COUNT_N.

4.3.4.3.2 Handover Failure

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

When AMS resuming communications with the serving ABS(MZone), it notifies the incremented current AMS AK_COUNT_M to the ABS using AAI-HO-IND message. The serving ABS SHALL then inform the Anchor Authenticator of this new value by using the R6 *CMAC_Key_Count_Update* message and the Authenticator SHALL re-sync its AK_COUNT_N accordingly, but legacy Authenticator may be not supporting that re-synchronization of AK_COUNT_N.

However, during the next (successful) reentry, HO, or secure location update, the MS/AMS will again increment its counter (X), this time to (N + 2), but if the Authenticator didn't synchronize with the incremented counter using AAI-HO-IND message, the target BS/ABS during the HO preparation phase will have its counter (Y) set to (N + 1) by the Authenticator. Nonetheless, when the target BS/ABS receives the RNG-REQ/AAI-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 $CMAC\_KEY\_COUNT_N/AK\_COUNT_N$ accordingly.

4.3.4.4 Process Flowchart

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

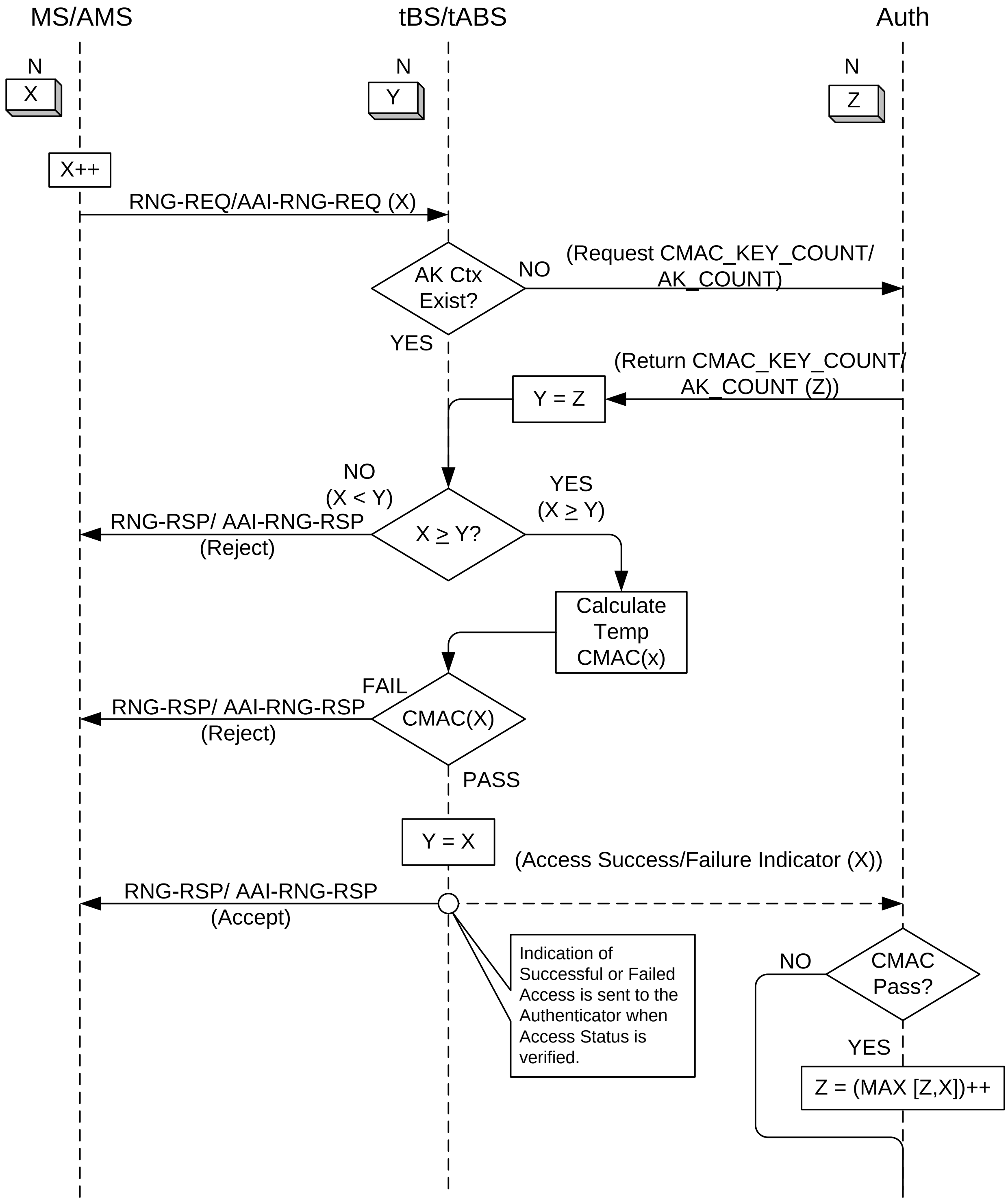

MS/AMS
tBS/tABS
Auth
N
X
N
Y
N
Z
X++
RNG-REQ/AAI-RNG-REQ (X)
AK Ctx Exist?
NO
(Request CMAC_KEY_COUNT/ AK_COUNT)
YES
(Return CMAC_KEY_COUNT/ AK_COUNT (Z))
Y = Z
NO (X < Y)
RNG-RSP/ AAI-RNG-RSP (Reject)
X ≥ Y?
YES (X ≥ Y)
Calculate Temp CMAC(x)
FAIL
RNG-RSP/ AAI-RNG-RSP (Reject)
CMAC(X)
PASS
Y = X
(Access Success/Failure Indicator (X))
RNG-RSP/ AAI-RNG-RSP (Accept)
Indication of Successful or Failed Access is sent to the Authenticator when Access Status is verified.
NO
CMAC Pass?
YES
Z = (MAX [Z,X])++

Figure 4-7 – 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/AMS. 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/AMS 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:

```
MN-HA-CMIP4 = H(MIP-RK,”CMIP4 MN HA” | HA-IPv4 | MN-NAI)
MN-HA-PMIP4 = H(MIP-RK,”PMIP4 MN HA” | HA-IPv4 | MN-NAI)
MN-HA-CMIP6 = H(MIP-RK,”CMIP6 MN HA” | HA-IPv6 | MN-NAI)
MAG-LMA-PMIP6=H(PMIP6-RK, “PMIP6 MAG LMA” | MAG-IPv6 | LMA-IPv6 | 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 PMIP-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:

```
FA-RK = H(MIP-RK,”FA-RK”)
MN-FA = H(FA-RK,”MN FA” | FA-IP | 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” | HA-IPv4 | FA-CoAv4 | 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:
    - the binary representation of the non null terminated string “FA-HA”
    - HA-IPv4 is a 32-bit binary representation of the IP address in network byte order
    - FA-CoAv4 is a 32-bit binary representation of the IP address in network byte order
    - 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 RRQs and MIP RRPs).

H()	HMAC-SHA1 [24]
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 4-8 illustrates the key distribution for CMIP4.

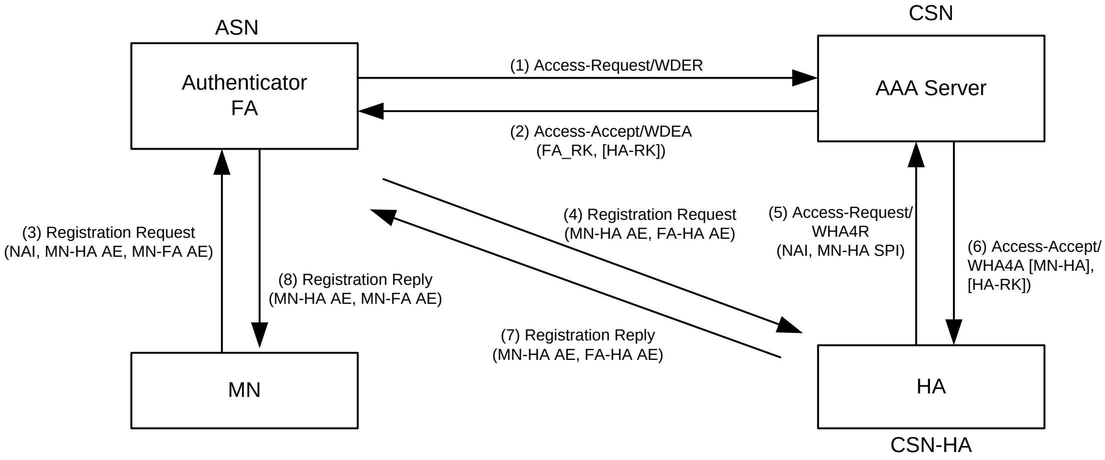


Figure 4-8 – CMIP4 Key Distribution without FA relocation

Note: Figure 4-8 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/AMS 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 exists) 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 4-8.

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

The following key distribution scheme applies:

The authenticator receives a set of mobility keys and other keys in the RADIUS Access-Accept packet or Diameter WDEA command as a result of successful authentication. These include FA-RK, and HA-RK (with its SPI and lifetime). MN-HA-CMIP4 SHALL NOT be sent to the authenticator by the HAAA. In the case of RADIUS, the keys are encrypted using the method defined in [43] section 3.5. In the case of Diameter, the keys are protected by the transport security mechanism (IPsec or TLS). The AAA messages MAY be transported through one or more AAA brokers or proxies. The keys are stored at the authenticator.

At the time of CMIP4 procedures, the FA obtains the MN-FA key and, if required, the FA-HA key it needs from the authenticator. If this is a new FA after re-location without re-authentication, the new FA requests the keys by sending a Context_Req message to the anchor authenticator if these keys are required. The FA SHALL set bit#8 in the Context Purpose Indicator TLV for requesting an MN-FA context, and bit#9 for requesting a FA-HA context. Upon receiving such Context_Req message from the FA, the anchor authenticator SHALL reply with a Context_Rpt message including a MIP4 Security Info TLV to carry the requested keys. 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.

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

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

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

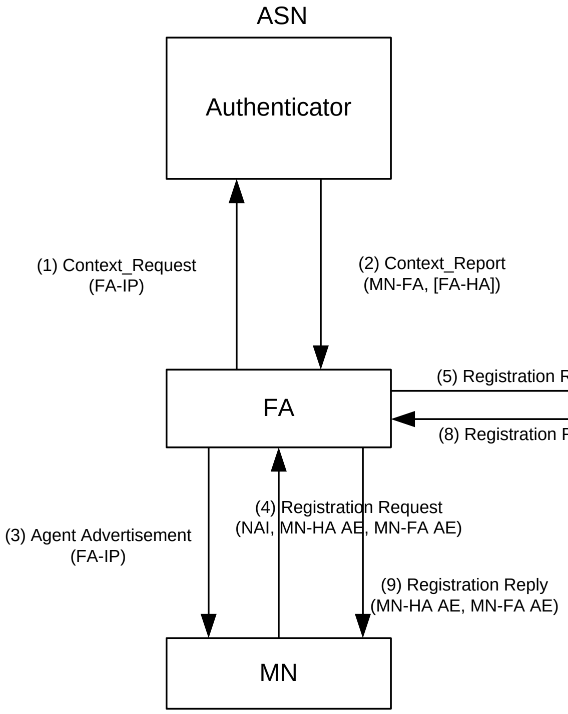

ASN
Authenticator
CSN
AAA Server
(1) Context_Request (FA-IP)
(2) Context_Report (MN-FA, [FA-HA])
(6) Access-Request/ WHA4R (NAI, MN-HA SPI)
(7) Access-Accept/ WHA4A [MN-HA], [HA-RK]
FA
HA
(5) Registration Request (MN-HA AE, FA-HA AE)
(8) Registration Reply (MN-HA AE, FA-HA AE)
CSN-HA
(3) Agent Advertisement (FA-IP)
(4) Registration Request (NAI, MN-HA AE, MN-FA AE)
(9) Registration Reply (MN-HA AE, MN-FA AE)
MN

Figure 4-9 – 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 4-10 illustrates the key distribution for PMIP4 operations.

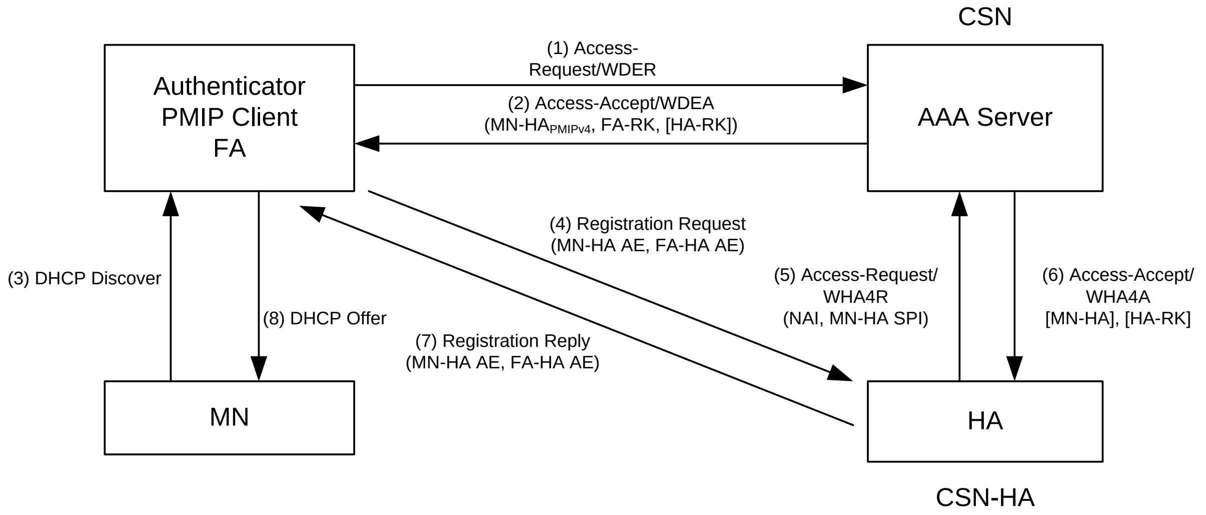

CSN
Authenticator
PMIP Client
FA
(1) Access-Request/WDER
(2) Access-Accept/WDEA (MN-HA$_{PMIPv4}$, FA-RK, [HA-RK])
AAA Server
(4) Registration Request (MN-HA AE, FA-HA AE)
(3) DHCP Discover
(8) DHCP Offer
(7) Registration Reply (MN-HA AE, FA-HA AE)
(5) Access-Request/ WHA4R (NAI, MN-HA SPI)
(6) Access-Accept/ WHA4A [MN-HA], [HA-RK]
MN
HA
CSN-HA

Figure 4-10 – PMIP4 Key Distribution

Note: Figure 4-10 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 exists) 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 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 [43] 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 [43] 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/AMS and the Home AAA server derive the MIP-RK key from the EMSK key resulting from the successful EAP authentication. Both the MS/AMS 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/AMS commences MIP6 procedures it obtains the MN-HA-CMIP6 key. It uses this key to authenticate the Binding Update packet as defined by [72].

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 [43] 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

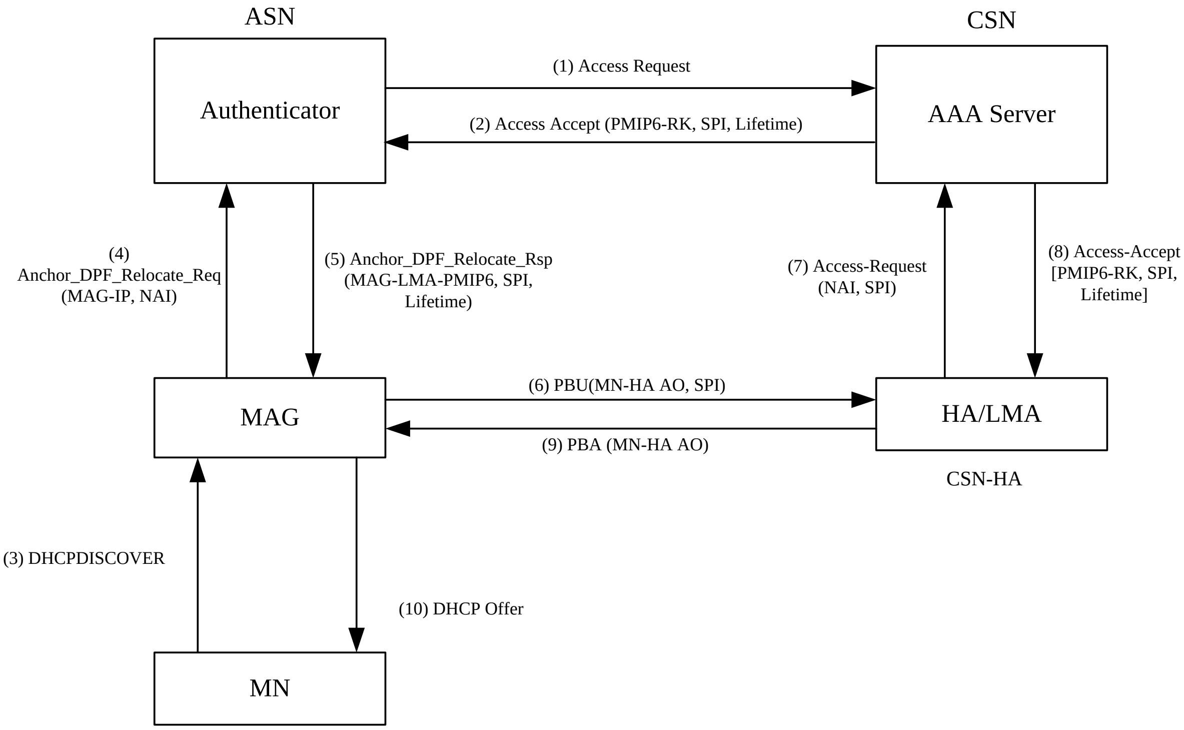

ASN
CSN
Authenticator
AAA Server
(1) Access Request
(2) Access Accept (PMIP6-RK, SPI, Lifetime)
(4) Anchor_DPF_Relocate_Req (MAG-IP, NAI)
(5) Anchor_DPF_Relocate_Rsp (MAG-LMA-PMIP6, SPI, Lifetime)
(7) Access-Request (NAI, SPI)
(8) Access-Accept [PMIP6-RK, SPI, Lifetime]
MAG
HA/LMA
(6) PBU(MN-HA AO, SPI)
(9) PBA (MN-HA AO)
CSN-HA
(3) DHCPDISCOVER
(10) DHCP Offer
MN

Figure 4-11 – PMIP6 Key Distribution

The MAG and the authenticator may be collocated or separated. Figure 4-11 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 exists) 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 4-11.

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 [43] 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 [43] 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 [72]. 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 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/AMS 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 [66]. 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 [66] 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.

DHCP-key = HMAC-SHA1(DHCP-RK, “DHCP AUTH” | DHCP-Relay-IP | 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/AMS 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 4-12 describes the distribution of DHCP keys for the case when the DHCP relay is collocated with authenticator:

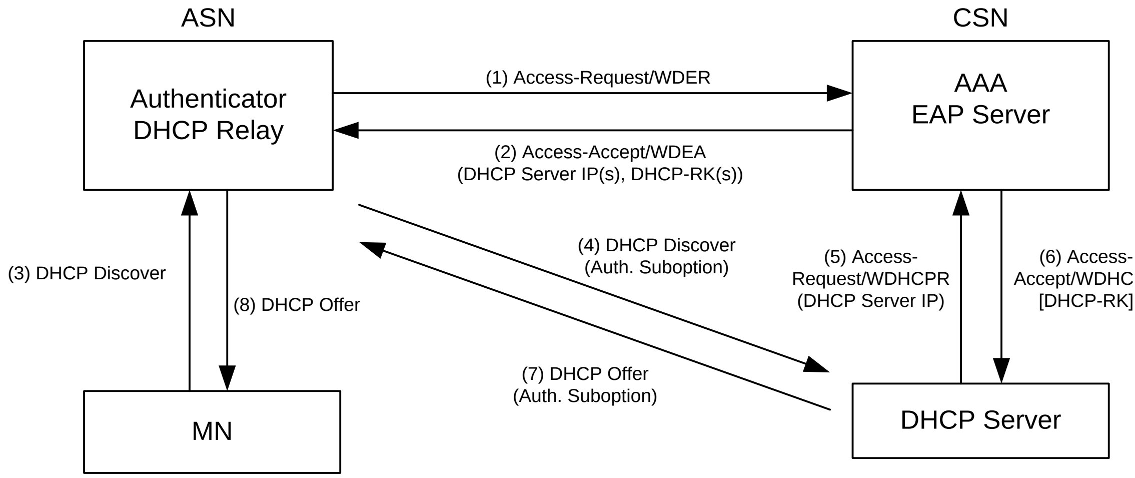


Figure 4-12 – Initial DHCP Key Distribution

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 [43] 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-SHA1as per [66] 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 [66]. 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 [66].

The DHCP server SHALL provide the DHCP response message with the authentication suboption, as per [66].

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

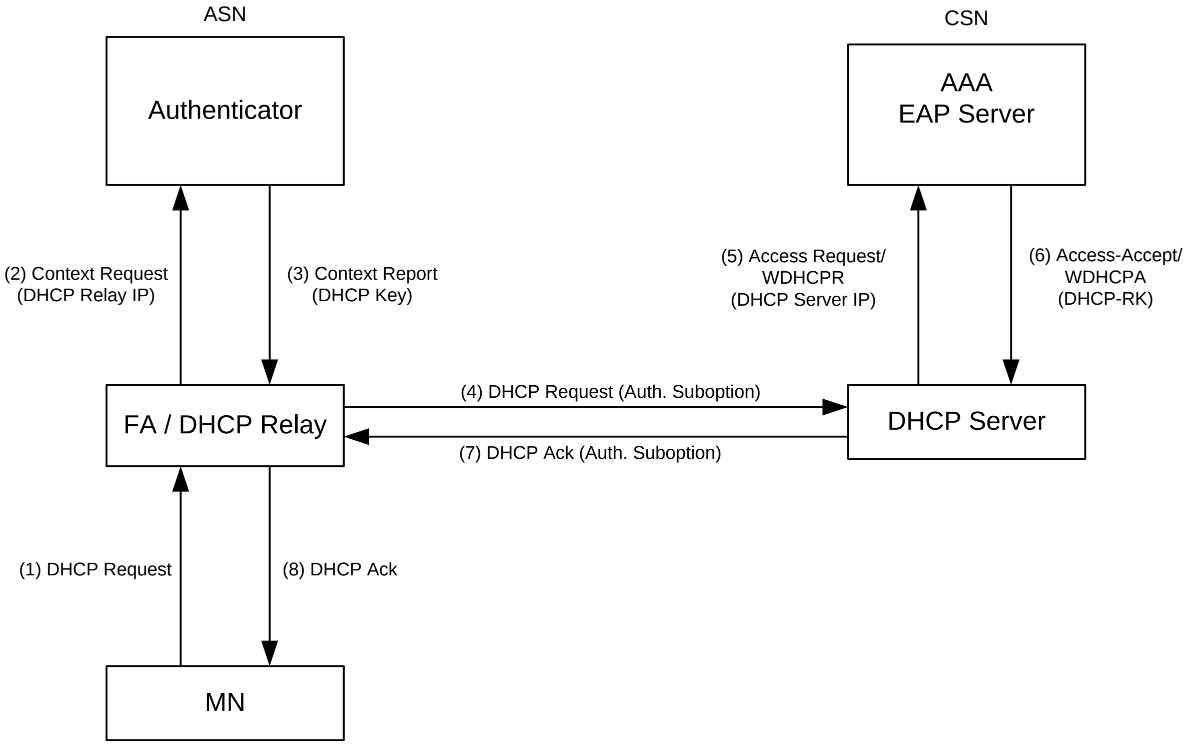


Figure 4-13 – DHCP Key Distribution when Authenticator and DHCP Relay are not collocated

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 [66] 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 4-6 – 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 4-7 – 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/AMS 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 [38]
- RFC 3579 [53]

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 [67].

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

Table 4-8 – Functional Blocks for Device/User Authentication

Entity	Function
MS/AMS	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.

Entity	Function
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/AMS authorization attributes, HAAA decides for the MS-Certified-Feature-List-For-GW and MS-Certified-Feature-List-For-BS based on the MS/AMS 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/AMS and the EAP authentication server uses [57] 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/AMS SHALL support EAP-TLS, as outlined in [17].

For user authentication, MS/AMS 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/AMS SHOULD check the revocation status of AAA server's X.509 certificate at the time of network access authentication. MS/AMS SHOULD use and HAAA SHALL support light-weight profile [87] of OCSP [60] over EAP-TLS [17] by means of TLS extensions.

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/AMS 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:

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

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

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

The EAP-TLS client in MS/AMS 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/AMS during EAP-TLS. The MAC address and Model SHALL be extracted from the X520CommonName RDN.

When MSID privacy is not applied, the MAC address 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.

But, when MSID privacy is applied to AMS, the MAC address SHALL be compared with the MAC address delivered via the first Accounting start message. If they do not match the authentication SHALL be rejected, and AMS is forced to exit the network.

If the MAC address matching is successful, the EAP method executes to completion. If the EAP method terminates with EAP-Failure, the MS/AMS, BS/ABS, and the authenticator SHALL perform the disconnection procedure as defined in [11]. Furthermore, if the MS/AMS received network rejection information via EAP Notification, then the MS/AMS SHALL act according to the section 4.5.1.4.

The MS/AMS 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.

If the EAP session is completed successfully (i.e. the MS/AMS receives PKMv2 SA_TEK_Challenge or PKMv3 Key_Agreement-MSG#1 message with a valid CMAC), the MS/AMS SHALL act depending on the realm match or the mismatch. In case of realm match, when receiving PKMv2 SA_TEK_Challange or PKMv3 Key_Agreement-MSG#1 message from the BS/ABS, the MS/AMS SHALL respond with PKMv2 SA_TEK_Request or PKMv3 Key_Agreement-MSG#2 message in order to continue the connection procedure. On the other hand, in case of realm mismatch, the MS/AMS SHALL reject the connection.

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 [23] 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.

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

4.4.1.2.2 EAP-AKA

When EAP-AKA is used for user authentication, MS/AMS 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/AMS 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/AMS 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:

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

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

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

The EAP-TTLS client in MS/AMS 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/AMS 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/AMS SHALL reject authentication.

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 [23] 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.

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

The AAA server SHALL parse the x.509 certificate if sent to it by the MS/AMS during EAP-TTLS. The MAC address and Model SHALL be extracted from the X520CommonName RDN.

The MAC address SHALL be compared with the MAC address in the Calling-Station-Id of the RADIUS Access-Request packet or Diameter WDER command when MSID privacy is not applied. If they do not match, the authentication SHALL be rejected.

But, when MSID privacy is applied, the MAC address SHALL be compared with the MAC address delivered via the first Accounting start message. If they do not match HAAA server SHALL trigger AMS de-registration.

4.4.1.2.4 Quick EAP

When an MSK and an EMSK are already shared between MS/AMS and HAAA, if its anchor authenticator needs to be relocated to a Rel.2.x ASN-GW from a Rel.1.x ASN-GW in some situations(e.g. a L-to-M handover from legacy BS indication). The following Quick EAP re-authentication is used in order to expedite the EAP re-authentication procedure in place of a normal EAP procedure. Note: The following is a quick EAP procedure since it uses the already generated MSK and as a result, the interaction with the AAA is minimized.

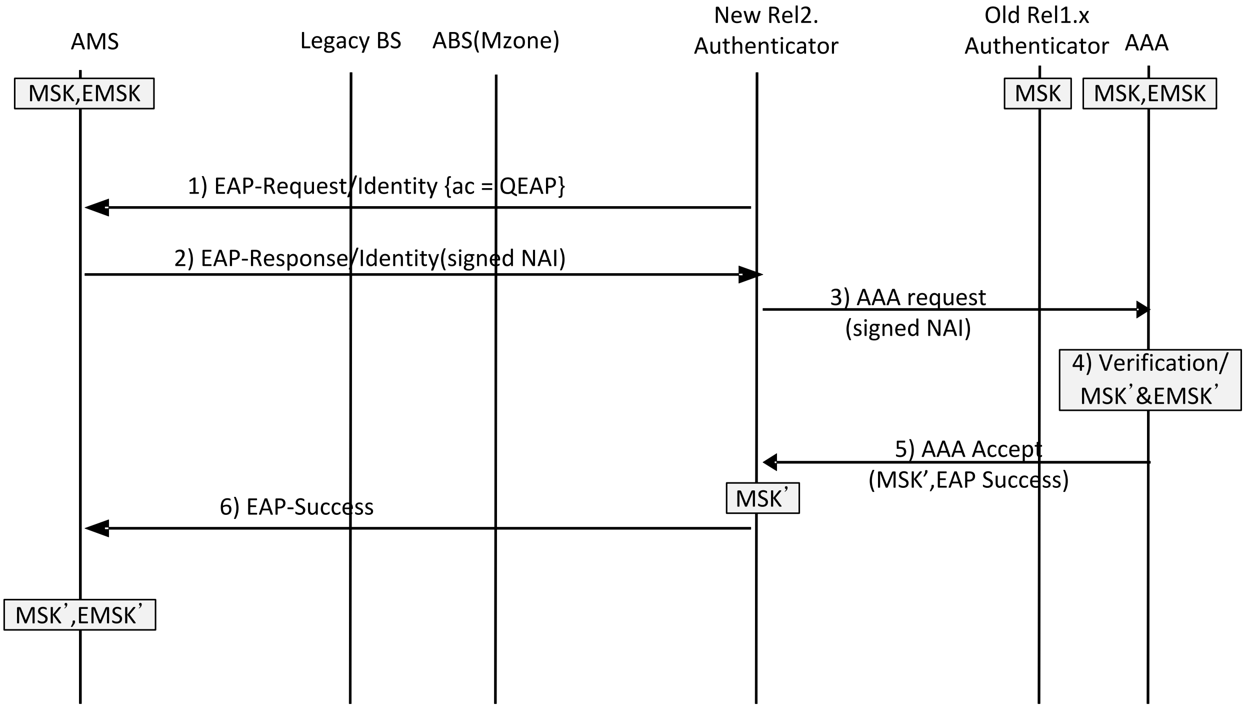


Figure 4-14 – Quick EAP-reauthentication with AA relocation during a L-to-M handover from legacy BS

STEP 1

The new Release 2.x Authenticator sends an *EAP-Request/Identity* message over AR_EAP_Transfer to initiate an EAP Phase, where Release 2.x Authenticator sets an authentication decoration {ac = QEAP} in the *EAP-Request/Identity* if the EAP re-authentication is for the authenticator relocation from Release 1.x authenticator during the L-to-M handover from legacy BS to a ABS(MZone). i.e. *EAP-Request/Identity*{ac = QEAP}; if {ac = QEAP} doesn't exist in the EAP-Request/Identity or the AMS doesn't support the quick EAP feature, the AMS shall perform the regular EAP (re)authentication.

STEP 2

Upon receiving the *EAP-Request/Identity* message with authentication decoration "OQEAP", the AMS sends an EAP-Response message including a signed NAI to the new Release 2.x Authenticator.

The format of the signed NAI is as follows:

{ac = ASCII print of Nonce1 - ASCII print of Nonce2 - ASCII print of EMSKhash} username@homerealm

,where it is a decorated NAI that includes a decoration called "ac" that carries an "authentication code". The decoration is followed by username and home realm portions of a standard NAI. Nonce1 and Nonce2 are 64-bit numbers that are generated by the AMS. Nonce1 is a monotonically-increasing number, and Nonce2 is a randomly-generated number. The very first Nonce1 value received for a given EMSK shall be 1. AMS shall perform a standard EAP authentication after the Nonce1 reaches the maximum possible value, so that it can be reset to 1 (and a new EMSK is generated as well). *EMSKhash* is defined by *EMSKhash* =HMAC-SHA256 (EMSK, Nonce1).

For example, a singed NAI is shown by

{ac=63456-23449-2349872510872345087234985234989273458925578654}joe@hnsp.com

STEP 3

Upon receiving the *EAP-Response/Identity* message the new Release 2.x Authenticator relays it to home AAA server over an AAA request message.

STEP 4

The home AAA server verifies the *EMSKhash* received in the signed NAI.

The home AAA server needs to ensure Nonce1 value is a fresh one. For that purpose the home AAA server stores the previously used Nonce1 value to make sure the next value is greater than the previous one throughout the lifetime of an EMSK. If the home AAA server receives a Nonce1 value smaller than or equal to the previously used one, then it considers the verification as failed.

Subsequently received Nonce1 values don't have to be immediately following each other as some intermediate values may be lost in transmission. If the Nonce1 value is a fresh one, home AAA server replaces the stored value with the new one for the future replay prevention. When the EMSK expires, its nonce store is flushed along with that.

If the verification fails, the home AAA server falls back to following the standard (and lengthy) procedure by executing an appropriate EAP method (e.g., EAP-TLS, EAP-AKA, etc.).

If the EMSKhash verification succeeds, the home AAA server computes the new MSK and EMSK values to be used according to the following formulas:

MSK' = HMAC-SHA256 (MSK, Nonce2)

EMSK' = HMAC-SHA256 (EMSK, Nonce2)

STEP 5

EAP success message and MSK' are sent to the new Release 2.x Authenticator over an AAA Accept message.

STEP 6

EAP success message is relayed to the AMS. Upon receiving it, the AMS computes the new MSK and EMSK values as same as the home AAA server using the same algorithm described in Step 4 for the AAA.

4.4.1.3 Network Access Identifier

The Network Access Identifier (NAI) SHALL conform to [69]. 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/AMS 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 [65] and section 5.1 of [41]. 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/AMS 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 [69]. Example: hnsp1.com!joe@vnsp.com

WiMAX decoration: Optionally used to indicate various MS/AMS 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 [69]. The name must be alphanumeric with no spaces.

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

The MS/AMS SHALL decorate the NAI with the CRN. The NAI decoration SHALL be based on AVP definition as per Table 4-9. The network uses the CRN value as a key with which it accesses the CVS data-base to obtain certification information associated with the MS/AMS.

If the MS/AMS is a WiMAX device which is embedded in a platform (laptop PC with an embedded WiMAX device – for example) it decorates the NAI with the EPID in addition to the CRN as per Table 4-9. The CRN is a 6 character alphanumeric ASCII string all uppercase. The EPID is an 8 byte value represented as 16 ASCII HEX characters all uppercase (See [7] for additional information). In this case, the network concatenates the CRN and EPID values to perform the key with which it accesses the CVS data-base (CRN value on the left hand side and EPID value on the right hand side).

Example of a NAI generated by an MS/AMS:

{crn=TUV123}User_ID@Realm

The string used by the HAAA to locate the certification information is TUV123.

Example of a NAI generated by a platform with an embedded WiMAX device:

{crn=TUV123|epid=001ABF6547DE9876}User-ID@Realm

The string used by the HAAA to locate the certification information is: TUV123001ABF6547DE9876.

Currently the following AVPs are defined:

Table 4-9 – 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]
epid	Embedding Platform ID value expressed in ASCII hex values	Carries the platform ID value for Certification Version signaling (CVS)	This document.
crn	Certification Registration Number (CRN) expressed in ASCII uppercase alpha numeric assigned to the MS/AMS 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 4-9 are reserved.

The AAA server SHALL ignore any AVP in a WiMAX decoration that it does not recognize.

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/AMS SHALL generate a pseudo-identity to be used as the username in the Outer-Identity.

realm: As specified by [69]. 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@hnsp.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/AMS requirements for generating pseudo-identities are as follows:

- If the MS/AMS is required to generate a pseudo-identity, then the MS/AMS SHALL generate a fresh pseudo-identity for each network entry.
- To reduce the probability of identity collisions, the pseudo-identity generated by the MS/AMS SHALL be at least 128-bit random number, expressed in ASCII-hex. For example the resulting random pseudo-identity is: A234F6789B123456123456789C12345E. Note: the random number generator needs to be seeded by a value that is not common to multiple MSs. Such value for example would be time, or the MAC address of the device.

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/AMS in the realm of the HCSN. If the pseudo-identity is used by another MS/AMS, 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/AMS 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/AMS (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 ([72]).

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/AMS and the ASN using PKM messages, which are PKMv2 or PKMv3 depending on the applied 802.16 air interface.

ASN selects Single EAP during SBC negotiation.

Network access authentication is started when the MS/AMS 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/AMS. Details of how MS/AMS learns this policy is outside the scope of this specification.

The MS/AMS 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/AMS.

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

After successful completion of the authentication, the MS/AMS SHALL compute the keys required for PKMv2 or PKMv3 using the MSK. The MS/AMS SHALL use the EMSK to compute other application keys (see section 4.3.1).

In response to an EAP Success message, the MS/AMS is granted access to the network and SHALL proceed either with PMIP or CMIP procedures. As well, the MS/AMS 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/AMS 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/AMS 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/AMS encounters a new OCSP responder, the MS/AMS SHOULD download the OCSP CRL using HTTP after the network access is granted. If the MS/AMS discovers that OCSP responder's certificate is listed as revoked in the CRL, then the MS/AMS SHALL regard the network access authentication procedure as failed and initiate network exit procedure. If the MS/AMS 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 HNSP requires to authenticate/re-authenticate the subscriber credential only, an appropriate EAP method that can use subscriber credential SHALL be selected and executed between the MS/AMS and the HCSN. When the subscriber is identified by the MAC address of the MS/AMS, device credential can be used as the subscriber credential.

If an EAP authentication that relies on availability of subscriber credentials on the MS/AMS (e.g., EAP-TTLS with MSCHAPv2) does not successfully complete, the MS/AMS SHALL retry authentication for a finite number of times (e.g., 3). If the successful authentication is not achieved after the last attempt, in the next attempt the MS/AMS SHOULD offer the network to connect using EAP-TLS by sending EAP-Response NAK in response to the EAP method requested by the network and suggest its preferred EAP method as EAP-TLS. The NAI used by the MS/AMS in this EAP exchange is implementation specific and can be chosen by MS/AMS from the NAI defined for the original method or the one defined for EAP-TLS. Falling back to TLS does not mean the MS/AMS falls back to non-provisioned mode. Hence, the NAI is not expected to include the {sm=1} decoration. This scheme allows the MS/AMS to enter the network for treatment using X.509 device certificate based authentication (i.e., without the subscriber credentials such as username and password). The network's decision on whether to agree to EAP-TLS and the treatment of the MS/AMS is beyond the scope of this specification. For example, the network may refuse to perform EAP-TLS if it was able to authenticate the subscriber credentials and therefore assumes the fail is due to RF conditions or an attack. When the MS/AMS is allowed to enter the network under this circumstance, the network SHOULD provide limited access service to the MS/AMS.

This MS/AMS behavior definition does not change the HNSP state and configuration parameters within the MS/AMS but just defines the specific one-time behavior expected from the MS/AMS in this scenario. The MS/AMS behavior (such as trying again with original EAP method, trying to connect to another NSP, etc.) in case the EAP-TLS authentication does not complete successfully is implementation specific and beyond the scope of this specification.

4.4.1.4.1.1.2 Authenticating Subscriber and Device Credentials

A HNSP 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/AMS 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/AMS 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 [55] 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/AMS (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/AMS network access.

The NAS SHALL act as an EAP pass-through ([57]) 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/AMS.

Upon receiving an RADIUS Access-Reject or Diameter WDEA with EAP-Failure indication, the NAS SHALL deny the MS/AMS 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/AMS 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 [53] 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, if MSID privacy is not applied, but the NAS shall include MSID* in the Calling-Station-Id if MSID privacy is applied.

c.f. The NAS SHALL include the MS MAC address in the first Accounting start message if MSID privacy is applied.

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.

4.4.1.4.2.2.2 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/AMS.

4.4.1.4.2.2.3 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/AMS network access.

As per [53], 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/AMS.

The NAS SHALL store the MSID* of the AMS if the MSID privacy is applied.

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/AMS 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.

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

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

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

The MS/AMS 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/AMS 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.

4.4.1.4.2.2.4 NAS Receives Final Access-Reject

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

The NAS SHALL validate the Message-Authenticator (80) attribute as per [53]. The NAS SHALL silently discard the Access-Reject packet if the Message-Authenticator attribute is not present or the computed Message Authenticator does not match the value received in the Access-Reject packet.

4.4.1.4.2.3 Diameter Message Processing

4.4.1.4.2.3.1 DER

The NAS SHALL send a WDER command as triggered by the EAP process to initiate authentication. The NAS SHALL follow the procedures defined in RFC4072 [67] with the following clarification:

- The NAS SHALL include the WiMAX-Capability AVP as describe in section 5.5.2.1.
- The NAS SHALL set the EAP-Payload attribute to the value received in the EAP-Response/Identity from the MS/AMS,
- The NAS SHALL set the value of the Calling-Station-ID AVP to the MS's MAC address if MSID privacy is not applied. The NAS SHALL set the value of the Calling-Station-ID AVP to the AMS's MSID* if MSID privacy is applied.
- If the NAS supports CUI and it requires CUI to be delivered by the HAAA, then the NAS SHALL include the CUI attribute in the WDER command and SHALL set its value to a single ASCII NUL character.

- The NAS SHOULD forward the WDER packet to the VAAA in the visited CSN using the routing decoration of the NAI, if any.
- During EAP authentication process when the NAS acts in pass through mode, the NAS MUST validate the EAP header fields as specified in RFC4072 [67].
- If the NAS supports fixed and nomadic access, it SHALL include either the serving BS-ID or the serving BS Location AVP, or both, in the Diameter WDER command.

4.4.1.4.2.3.2 DEA

EAP authentication requires multiple AAA transactions, that is, the NAS will receive WDEA command with Result-Code AVP set to “DIAMETER_MULTI_ROUND_AUTH”. Processing of these messages conform to the RFC4072 [67].

During EAP processing the NAS acts in passthrough mode and MUST validate the EAP header fields contained in the EAP-Payload AVP as defined by RFC4072 [67].

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

If the WDEA command indicates failure the NAS SHALL forward the contents of the EAP message to the MS/AMS and disallow the MS/AMS WiMAX Network Access.

If the final WDEA command does not contain the EAP-Master-Session-Key AVP, then the NAS MUST treat the response as a rejection and disallow WiMAX network access.

If the NAS required the inclusion of the CUI attribute and the final WDEA command does not contain the CUI attribute then the NAS MUST treat the response as a rejection and disallow WiMAX network access.

If the WDEA command includes all the needed attributes and indicates success, the NAS SHALL forward the contents of the EAP message to the MS/AMS. This marks the start of the WiMAX session for the MS/AMS.

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

If the NAS received a set of attributes for Mobile IP procedures it 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. One 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 attribute allocated by VAAA is applied; otherwise, if HA in home network is selected, the HA attribute allocated by HAAA is 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 Diameter Accounting-Request command.

The NAS SHALL store the first Class attribute if received in the Diameter WDEA associated with the network access authentication.

The NAS SHALL store the WiMAX-Session-Id attribute received in the WDEA command. The WiMAX-Session-Id SHALL be used in all subsequent WDER commands. The WiMAX-Session-Id is also sent in the Diameter Accounting commands. Note that the WiMAX-Session-Id is different than the Diameter Session-ID. The Diameter Session-Id is established by the NAS and is unique to the NAS/AAA. Whereas the WiMAX-Session-Id is established for the WiMAX network access authentication session.

If received, 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 also be used by the PMIP client to set the PMIP NAI.

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.

If the NAS supports fixed and nomadic access, then it SHALL store the Mobility access Classifier if received in the Diameter WDEA. If the NAS does not support fixed and nomadic access then it SHALL ignore the Mobility access Classifier if received in the WDEA command.

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

If the NAS supports only fixed and nomadic access, then a mobility access classifier of Mobile received in the Diameter WDEA command may be treated as a nomadic access classifier or denied service based on the NAS local policy.

The NAS SHOULD initiate MS network exit for any MS/AMS using the same MAC address as the one that is newly authenticated by the WDEA command received from the HAAA, unless the MS/AMS already residing in the network performed device authentication during initial network entry and has an authenticated MAC address, but the newly authenticated MS/AMS did not perform device authentication (indicated by the value of the MS-Authenticated AVP, if present in the WDEA command from the HAAA).

The MS/AMS 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/AMS 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 [55] 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 an 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 [55] and advertise support for the "WiMAX Network Access Authentication and Authorization Diameter Application" (see section 5.5.1.1).The VAAA MAY acts 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 [53]. Similarly, a Diameter AAA Proxy SHALL conform to RFC4072 [67]. 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 [69] and route the RADIUS packets accordingly. When using Diameter routing is performed based on RFC3588 [55].

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 exchanges. 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 [55] 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 [67]).

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.

When the MSID privacy is not applied, 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.

But, when the MSID privacy is applied, the HAAA SHALL verify that the MS MAC address (not MSID*) received in the first accounting start message from the Authenticator does not match the MS MAC address (not MSID*) 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/AMS 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/AMS 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. The HAAA MAY delete the MSK key after sending the Access-Accept packet to the NAS. Note that the generated MSK may be required at the AAA later on during the session if the AAA supports the Optimized Combined Relocation (OCR) feature, see section 4.20 and/or the Quick EAP feature, see section 4.4.1.2.4.

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/AMS.

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/AMS is attaching to a NAP to which the HNSP 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/AMS 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/AMS 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/AMS 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/AMS 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/AMS.

If the NAI does not contain a WiMAX decoration with an IPID AVP, the HAAA SHALL assume that this MS/AMS does not support Certificate Version Signaling (CVS). The HAAA will decide based on operator policy whether or not to grant access to such MSs/AMSs.

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 [53] 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/AMS 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 [53] 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 0.

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 5-29.

The HAAA SHALL compute the values of the mobility keys as described in sections 0 and 4.3.5.

Upon successful network access authentication, when MSID privacy is not applied, the HAAA SHOULD initiate MS/AMS network exit for any existing WiMAX session with an MS/AMS 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).

But, when MSID privacy is applied, on receiving the first accounting start message from the Authenticator, the HAAA SHOULD initiate MS/AMS network exit for any existing WiMAX session with an MS/AMS using the same MAC address as indicated in the first accounting start message 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 an MS/AMS 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/AMS 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/AMS 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 [53] 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 [55] 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 [55].

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.

Note that depending on the applied PKM version some parameters and messages are differently defined but for similar usage (e.g. Authorization Grace time and Authentication Grace time, CMAC_KEY_COUNT and AK_COUNT, PKMv2 EAP-start and PKMv3 Reauth-Request, etc. in PKM v2 and v3 respectively).

4.4.1.5.1 Reauthentication Triggers

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

MS/AMS 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/AMS.

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

- "Authorization Grace Time" in PKMv2 or "Authentication Grace Time" in PKMv3 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 in PKMv2 and 2^24 -10000 in PKMv3);
- "CMAC_KEY_COUNT Grace Interval" in PKMv2 or "AK_COUNT Grace Interval" in PKMv3 is reached (CMAC_KEY_COUNT or AK_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:

- "Authorization Grace Time" in PKMv2 or "Authentication Grace Time" in PKMv3 is reached (the pre-configured time elapses before PMK lifetime expires);
- "CMAC_KEY_COUNT Grace Interval" in PKMv2 or "AK_COUNT Grace Interval" in PKMv3 is reached (CMAC_KEY_COUNT or AK_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/ABS (*AR_EAP_Start* message with BS-originated trigger TLV) informing it that MS/AMS' security context in the BS/ABS is going to expire (AK Context in a BS/ABS, CMAC_PN_* counters, etc.);
- Authenticator receives *AR_EAP_Start* message from the Serving BS/ABS (in the case the MS/AMS instigates reauthentication by sending protected PKMv2 EAP-Start or PKMv3 Reauth-Request 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 PKMv2 EAP-Start or PKMv3 Reauth-Request from MS/AMS 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/ABS (e.g., MS/AMS instigates reauthentication by sending protected PKMv2 EAP-Start or PKMv3 Reauth-Request message and the Serving BS/ABS 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/AMS, "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 or PKMv3 EAP-Transfer message with EAP-Success payload is sent to the MS/AMS.

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/ABS detects PKMv2/PKMv3 3WHS successful completion and the "next" security key enforcement). During this "overlapping period", the ASN SHALL handle two security contexts for the MS/AMS - the "old" (currently active) and the "next" one.

Note, that Serving BS/ABS is not aware of EAP phase, it just relays EAP payload between PKMv2/PKMv3 EAP-related messages (protected by CMAC/AES-CCM based on the currently available AK) and AuthRelay protocol. EAP process is handled by Supplicant function in MS/AMS, 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/ABS, however, handles the location of the MS/AMS' Authenticator (Authenticator ID). In the case of Authenticator relocation scenario, the BS/ABS SHALL handle both IDs – the "old" Authenticator and the "new" one.

4.4.1.5.2.3 PKMv2/PKMv3 3-way Handshake (3WHS) Phase

PKMv.2/PKMv3 3-way Handshake (3WHS) process SHALL be performed after EAP phase completion to enforce the "next" PMK context. The Authenticator triggers PKMv2/PKMv3 3WHS start in the Serving BS/ABS by sending *Key_Change_Directive* message including the "next" security context. After the Serving BS/ABS detects the successful completion of the PKMv2/PKMv3 3WHS and ensures that the MS/AMS uses the new security context over the air, the BS/ABS sends *Key_Change_Cnf* message to the Authenticator including Key Change Indicator TLV, thus indicating the completion of PKMv2/PKMv3 3WHS and the enforcement of the "next" security context.

At this moment, the Serving BS/ABS deletes the "old" MS' security context and, in the case of Authenticator relocation, the Serving BS/ABS 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/PKMv3 3way handshake between BS/ABS and MS/AMS. 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/AK_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/AMS.

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/AMS, 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.

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

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

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

4.4.1.5.4 Reauthentication Process Without Authenticator Relocation

EAP-based Reauthentication always starts from Authenticator/ ASN GW by sending EAP-Request/ Identity message over *AR_EAP_Transfer* to Serving BS/ABS. MS/AMS instigates the start of Reauthentication in the Network by using PKMv2 EAP-Start or PKMv3 Reauth-Request message protected with CMAC digest (using the currently active AK). Except for “EAP-Start”/ “Reauth-Request’ steps, MS-initiated and Network-initiated Reauthentication procedures (without involving Authenticator relocation) are the same. The Serving BS/ABS MAY instigate the start of Reauthentication (e.g., if it detects that MS security context in BS/ABS is going to expire), by issuing *AR_EAP_Start* message to the Authenticator.

The MS Reauthentication process not involving Authenticator relocation is shown in Figure 4-15:

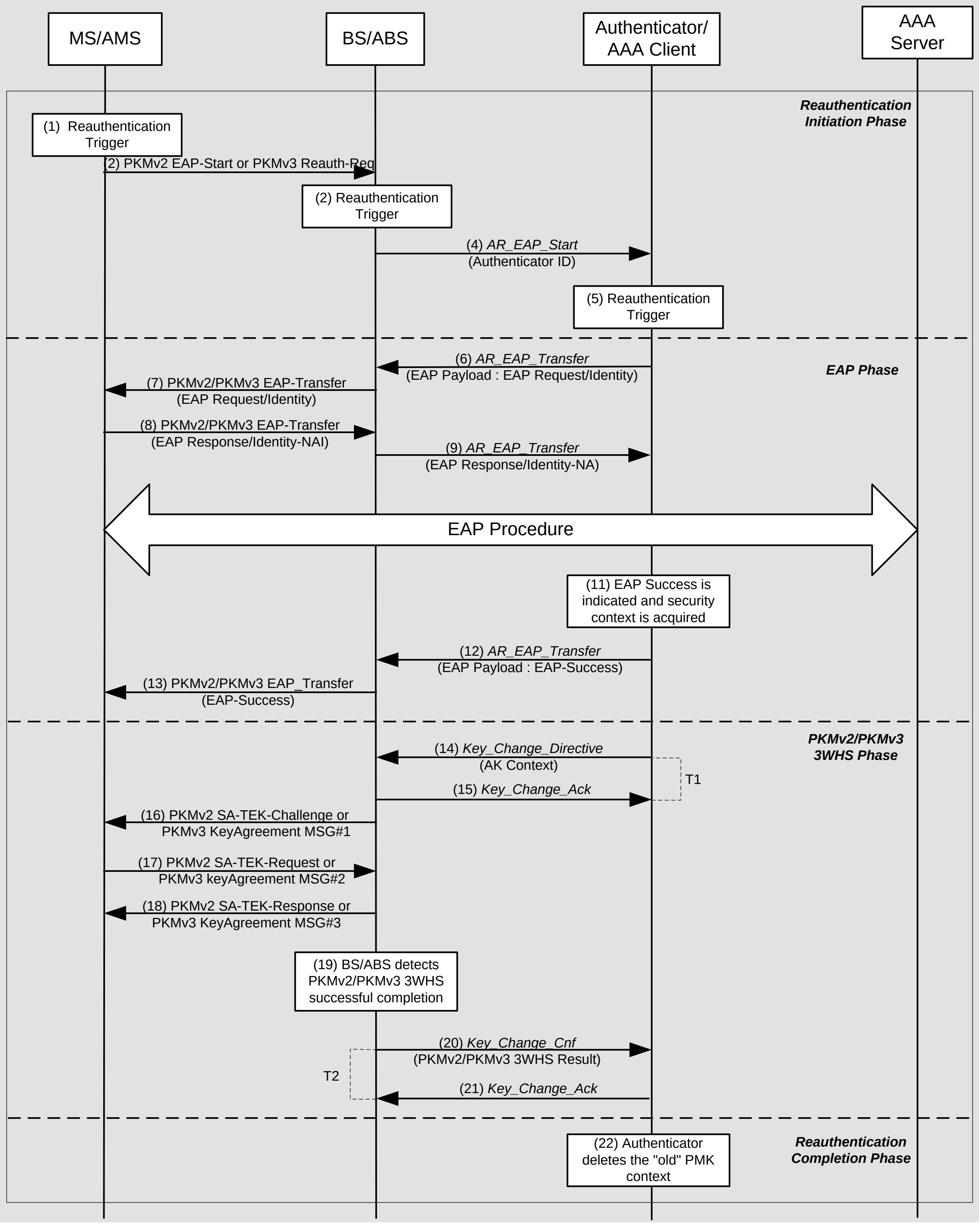

MS/AMS
BS/ABS
Authenticator/ AAA Client
AAA Server
Reauthentication Initiation Phase
(1) Reauthentication Trigger
(2) PKMv2 EAP-Start or PKMv3 Reauth-Req
(2) Reauthentication Trigger
(4) AR_EAP_Start (Authenticator ID)
(5) Reauthentication Trigger
EAP Phase
(6) AR_EAP_Transfer (EAP Payload : EAP Request/Identity)
(7) PKMv2/PKMv3 EAP-Transfer (EAP Request/Identity)
(8) PKMv2/PKMv3 EAP-Transfer (EAP Response/Identity-NAI)
(9) AR_EAP_Transfer (EAP Response/Identity-NA)
EAP Procedure
(11) EAP Success is indicated and security context is acquired
(12) AR_EAP_Transfer (EAP Payload : EAP-Success)
(13) PKMv2/PKMv3 EAP_Transfer (EAP-Success)
PKMv2/PKMv3 3WHS Phase
(14) Key_Change_Directive (AK Context)
T1
(15) Key_Change_Ack
(16) PKMv2 SA-TEK-Challenge or PKMv3 KeyAgreement MSG#1
(17) PKMv2 SA-TEK-Request or PKMv3 keyAgreement MSG#2
(18) PKMv2 SA-TEK-Response or PKMv3 KeyAgreement MSG#3
(19) BS/ABS detects PKMv2/PKMv3 3WHS successful completion
(20) Key_Change_Cnf (PKMv2/PKMv3 3WHS Result)
T2
(21) Key_Change_Ack
Reauthentication Completion Phase
(22) Authenticator deletes the "old" PMK context

Figure 4-15 – Reauthentication Procedure (w/o Authenticator Relocation)

STEP 1

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

STEP 2

MS/AMS sends PKMv2 EAP-Start or PKMv3 Reauth-Req 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/ABS, e.g., the BS/ABS detects that MS security context (AK lifetime, CMAC_PN_* counters, etc.) are going to expire. This step is relevant only when a BS/ABS instigates Reauthentication process.

STEP 4

Serving BS/ABS verifies CMAC digest of the received PKMv2 EAP-Start or PKMv3 Reauth-Req 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/ABS "relays" only protected and successfully verified PKMv2 EAP-Start or PKMv3 Reauth-Req messages. Unprotected (without CMAC digest) or "fail to verify" messages (with wrong CMAC digest) SHALL be discarded by a BS/ABS.

In the case reauthentication trigger occurs in a BS/ABS, the BS/ABS MAY issue *AR_EAP_Start* message by itself (without receiving PKMv2 EAP-Start or PKMv3 Reauth-Req from an MS/AMS). 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/ABS sending the AR_EAP_Start message no value is assigned by the BS/ABS yet for this R6 context of the MS/AMS (e.g. due a recent handover of the MS/AMS to this BS/ABS), the BS/ABS SHALL assign a value for this R6 context of the MS/AMS and SHALL populate R6_Context_ID with this value. Assignment of the value is internal to the BS/ABS. However, the value SHALL uniquely identify this context of the MS/AMS at this BS/ABS. The BS/ABS 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/ABS.

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

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

The composition of *AR_EAP_Start* message is presented in Table 4-10:

Table 4-10 – AR_EAP_Start

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS/AMS R6 context identifier
MS Info	5.3.2.103	O	Contains MS/AMS-related context in the nested IEs.

IE	Reference	M/O	Notes
>Authenticator ID	5.3.2.19	O	Contains the ID of the current MS/AMS Anchor Authenticator (the "old" Authenticator ID). This parameter may be omitted if the destination entity of the message is the current MS/AMS Anchor Authenticator (the "old" Authenticator) – i.e., there is no Authenticator relocation.
>BS-originated EAP-Start Flag	5.3.2.27	O	This flag is included when BS/ABS originates *AR_EAP_Start* message by itself (without receiving PKMv2 EAP-Start or PKMv3 Reauth-Req from an MS/AMS). This indicates BS-originated instigation of Reauthentication process (e.g., if MS security context in BS/ABS is going to expire).
BS Info	5.3.2.26	O	Contains relevant Serving BS/ABS context in the nested IEs.
> BS ID	5.3.2.25	CM	Serving BS ID. This TLV SHALL be included if BS Info is included in the transmitted message.

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/ABS. The composition of this message is presented in Table 4-11:

Table 4-11 – AR_EAP_Transfer from Authenticator to BS/ABS (EAP Initiation)

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS/AMS R6 context identifier
EAP Payload	5.3.2.62	M	EAP message. In this step it SHALL include EAP Identity Request message.
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	

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/ABS 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/ABS does not support the TLV, and SHALL not add the R6_Context_ID TLV in further R6 messages for this MS/AMS to the BS/ABS.

STEP 7

The Serving BS/ABS "relays" EAP-Request/ Identity payload to MS/AMS over PKMv2 EAP-Transfer message protected by CMAC digest or PKMv3 EAP-Transfer message protected by AES-CCM encryption (using the currently active AK context).

If the BS/ABS receives an R6_Context_ID TLV in AR_EAP_Transfer with the value set to zero, the BS /ABS SHALL assign a value for this R6 context of the MS/AMS 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/ABS. Calculation of the value is internal to the BS/ABS.

If the BS/ABS receives an AR_EAP_Transfer message without an R6_Context_ID value from the authenticator, the BS/ABS 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.

STEP 8

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

Under the situation that PKMv3 is applied: The AMS receives and verifies the PKMv3 EAP-Transfer message by decryption and if this verification is successful, transfers EAP payload to its EAP Supplicant layer. In response, AMS sends PKMv3 EAP-Transfer message with EAP-Response/ Identity payload (created by EAP Supplicant function in AMS), protected by AES-CCM encryption.

STEP 9

Under the situation that PKMv2 is applied: After the successful CMAC digest verification, Serving BS/ABS forwards EAP payload (EAP-Response/ Identity) of the received PKMv2 EAP-Transfer message to the Authenticator using *AR_EAP_Transfer* message.

Under the situation that PKMv3 is applied: Serving ABS forwards EAP payload (EAP-Response/ Identity) of the received PKMv3 EAP-Transfer message, which is verified by decryption, to the Authenticator using *AR_EAP_Transfer* message.

STEP 10

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

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 packets or Diameter WDER command containing the EAP payload.

The EAP authentication process (tunneling EAP authentication method) is performed between the MS/AMS and the Authentication server via the Authenticator in ASN GW in the same way as in the Initial Authentication. BS/ABS provides "relay" of EAP payload from PKMv2/PKMv3 EAP-related messages to AuthRelay and vice versa. The Authenticator in ASN GW acts in pass through mode (as described in [53]) and forwards the EAP messages received as a payload from the BS/ABS in AuthRelay 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 WDEA commands to AuthRelay. The composition of RADIUS packets is presented in section 5.4.1 and

Diameter commands in section 5.5.1.1. Service-Type attribute (type 6, [38]) is set to the value “Authenticate only” during reauthentication.

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

EAP peers (supplicant in MS/AMS 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/AMS and authentication server).

STEP 11

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

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

If Authenticator receives the RADIUS Access-Reject with EAP Failure indication or Diameter WDEA command with EAP-Failure encapsulated in the EAP-Payload AVP and Result-Code AVP indicating authentication failure, the Authenticator SHALL trigger the MS/AMS Network Exit as described in Table 4-25. 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/ABS as EAP Payload TLV in *AR_EAP_Transfer* message.

STEP 13

Under the situation that PKMv2 is applied: The BS/ABS relays EAP payload (received in AuthRelay message) to the MS/AMS 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/AMS the results of EAP process. Note, that the BS/ABS does not relate to the content of EAP Payload – whether it is EAP-Success or EAP-Failure message. The MS/AMS is also waiting for PKMv2 SA-TEK-Challenge message from BS/ABS to proceed with PKMv2 3way handshake.

Under the situation that PKMv3 is applied: The ABS relays EAP payload (received in AuthRelay message) to the AMS in PKMv3 EAP-Transfer/ AAI-PKM-RSP message protected by AES-CCM encryption (using the currently active AK context). This message indicates the Supplicant in the AMS the results of EAP process. Note, that the ABS does not relate to the content of EAP Payload – whether it is EAP-Success or EAP-Failure message. The AMS is also waiting for PKMv3 KeyagreementMSG#1 message from ABS to proceed with PKMv3 3way handshake.

STEP 14

The Authenticator sends *Key_Change_Directive* message to the BS/ABS to provide it with the “next” security context (AK Context) and trigger PKMv2/PKMv3 3WHS process between the BS/ABS and the MS/AMS (to enforce the “next” security context). The composition of this message is presented in Table 4-12:

Table 4-12 – Key_Change_Directive from Authenticator to BS/ABS

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS/AMS R6 context identifier.
BS Info	5.3.2.26	M	Contains BS/ABS-related context in the nested IEs.
>AK Context	5.3.2.6	O	This compound parameter includes AK context parameters (AK, AK SN/PMK SN, AK lifetime, etc.) for BS/ABS 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/PMK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.
>>CMAC_KEY_COUNT/AK_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 PKM2/3 message code.
>Authentication Result	5.3.2.18	M	
>PKM2/3 Message Code	5.3.2.134	M	
Certified-MS-Feature-List-for-BS	5.3.2.183	O[1]	Contains Allowed certified MS/AMS feature List for BS/ABS

Note [1]: 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/AMS Network exit as described in table 4-21.

STEP 15

BS/ABS receiving *Key_Change_Directive* message from Authenticator will acknowledge it by sending the *Key_Change_Ack* message.

STEP 16 - 18

The BS/ABS initiates PKMv2 3-way handshake (SA-TEK-Challenge/Request/Response exchange) or PKMv3 3-way handshake(Keyagreement MSG#1/#2/#3 exchange) with the MS/AMS to verify the new AK. The “next” security context (the “new” AK context) SHALL be used to protect PKMv2/PKMv3 3way handshake messages as specified in [11].

STEP 19

The BS/ABS detects the successful completion of PKMv2/PKMv3 3WHS process. The BS/ABS SHALL ensure that PKMv2/PKMv3 3way handshake is indeed successfully completed and the new PMK/AK is enforced by the MS/AMS – i.e., the BS/ABS should receive and verify a MAC management message from the MS/AMS signed by CMAC derived from the new AK. When BS/ABS recognizes the completion of PKMv2/PKMv3 3-way handshake process (success or failure), it SHALL indicate this event to Authenticator.

STEP 16

The BS/ABS indicates the completion of PKMv2/PKMv3 3WHS and enforcement of the "new" keys to the Authenticator by sending *Key_Change_Cnf* message with Key Change Indicator TLV.

Table 4-13 – Key_Change_Cnf Message from BS/ABS to Authenticator (PKMv2/PKMv3 3WHS Completion)

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS/AMS R6 context identifier.
Failure Indication	5.3.2.69	O	
MS Info	5.3.2.103	M	Contains MS/AMS-related context in the nested IEs.
>Key Change Indicator	5.3.2.86	M	Indicates the completion of PKMv2/PKMv3 3way handshake to Authenticator. In the case of successful PKMv2/PKMv3 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/ABS detects a failure of PKMv2/PKMv3 3WHS process for any reason, it sends *Key_Change_Cnf* message with Key Change Indicator TLV Result set to indicate "failure".

STEP 17

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

Table 4-14 – Key_Change_Ack

IE	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS/AMS R6 context identifier.
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	
Failure Indication	5.3.2.69	O	

STEP 20

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/AMS Anchor Authenticator. Optionally FA relocation can be done along with Authenticator relocation. This may occur in the following scenarios:

- In the case MS/AMS instigates Reauthentication process by PKMv2 EAP-Start or PKMv3 Reauth-Req message and the BS/ABS sends *AR_EAP_Start* message to its "default" Authenticator entity, which is different from the "old" Authenticator (the current MS/AMS 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/AMS 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/ABS. This means that MS/AMS has sent a protected PKMv2 EAP-Start or PKMv3 Reauth-Req message (signed by CMAC), BS/ABS has successfully verified it according to the currently active AK context and sent *AR_EAP_Start* message to the ASN GW (where the "new" Authenticator entity is located).
- In the case the Serving ASN triggers Reauthentication by itself, it is aware whether MS/AMS 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/AMS-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/ABS 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 or its later version Rel 2.0).

4.4.1.5.5.1.1 New Authenticator (WiMAX-Release “1.0” ASN) PULLs from Old Authenticator (WiMAX-Release “1.5” or its later version, “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” or its later version) 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” or its later version, “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” or its later version, “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” or its later version, “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” or its later version ASN)

“New” Authenticator (WiMAX-Release “1.5” or its later version ASN) rejects the PUSH procedure.

4.4.1.5.5.2 Authenticator Relocation - “PULL” Mode

Authenticator relocation “pull” mode is considered when:

- MS/AMS or the Serving BS/ABS instigate Reauthentication process and the Serving BS/ABS 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 4-16 presents Authenticator relocation “pull” mode.

If reauthentication is triggered by MS/AMS or BS/ABS, BS/ABS forwards *AR_EAP_Start* to the “new” Authenticator. In this case, BS/ABS SHALL include Old authenticator ID with *AR_EAP_Start* message.

Triggering of FA relocation is outlined in 4.4.1.5.5.

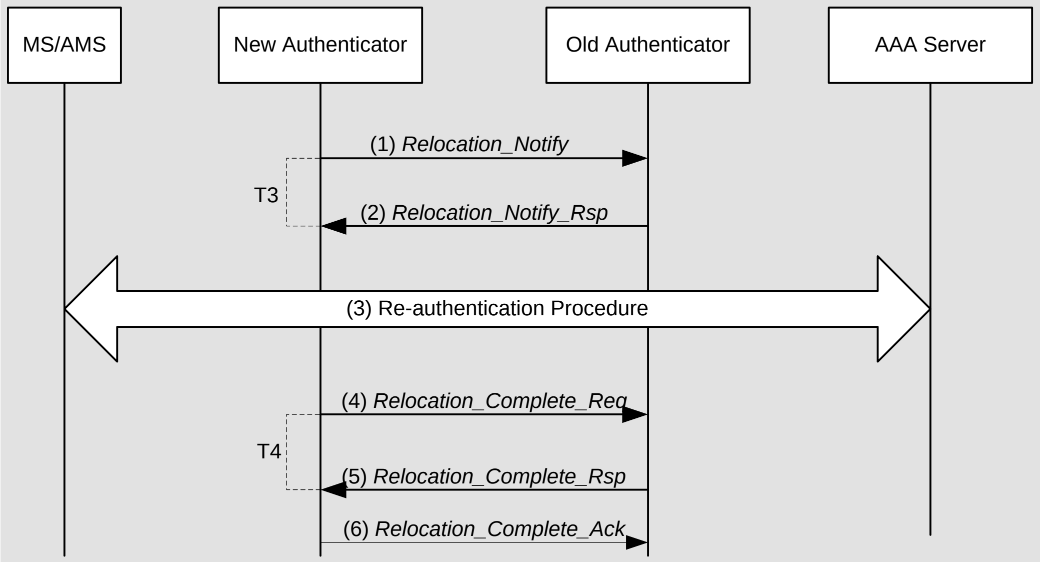

MS/AMS
New Authenticator
Old Authenticator
AAA Server
(1) Relocation_Notify
T3
(2) Relocation_Notify_Rsp
(3) Re-authentication Procedure
(4) Relocation_Complete_Req
T4
(5) Relocation_Complete_Rsp
(6) Relocation_Complete_Ack

Figure 4-16 – 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 4-15:

Table 4-15 – 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/AMS 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/AMS-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 18

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

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

1 **Table 4-16 – Relocation_Notify_Rsp from "Old" Authenticator to "New" Authenticator**

TLV	Reference	M/O	Notes	Applicability[4]
Failure Indication	5.3.2.69	O		1,2,3
Accept/Reject Indicator	5.3.2.1	M	Indicates Accept/ reject of the corresponding request.	1,2,3
MS Info	5.3.2.103	M	Contains MS/AMS-related context in the nested IEs.	1,2,3
>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.	1,2,3
>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.	1,2,3
> MS Security History	5.3.2.108	M	MS/AMS Security history – PMK SN.	1,2,3
>>PMK SN	5.3.2.133	M		1,2,3
>>MS NAI	5.3.2.105	M		1,2,3

[4] Note that from now on in this whole document Applicability Column represents each TLV's usability depending parameter negotiation between serving BS/ABS and old authenticator as follows.

1: network entry through Legacy BS and Legacy ASN GW

2: network entry through ABS(LZone) and Legacy ASN GW

3: network entry through ABS(MZone) and Advanced ASN GW

TLV	Reference	M/O	Notes	Applicability[4]
>>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.	1,2,3
>>Authorization Policy Support	5.3.2.21	M		1,2,3
>>VAAA IP Address	5.3.2.201	O	If the MS/AMS is re-authenticating via the visited CSN, either VAAA IP Address or VAAA Realm or both SHALL be included.	1,2,3
>> VAAA Realm	5.3.2.202	O	If the MS/AMS is re-authenticating via the visited CSN, either VAAA IP Address or VAAA Realm or both SHALL be included.	1,2,3
> MS Authorization Context	5.3.2.100	M	Contains Authorization context parameters of the specific MS/AMS.	1,2,3
>>MSID*	5.3.2.472	CM	Include when MSID privacy is applied.	3
>>MS NAI	5.3.2.105	M		1,2,3
>>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.	1,2,3
>>R3 WiMAX Capability	5.3.2.207	M		1,2,3
>>> R3 WiMAX-Release	5.3.2.441	M	WiMAX release negotiated during Initial Network Entry.	1,2,3

TLV	Reference	M/O	Notes	Applicability[4]
>>>R3 Accounting Capabilities	5.3.2.208	M	This TLV SHALL be included if R3 WiMAX-Capability is included in the transmitted message.	1,2,3
>>R3 CUI	5.3.2.210	O		1,2,3
>>R3 Class	5.3.2.211	O		1,2,3
>>R3 Framed IP Address	5.3.2.212	O		1,2,3
>>R3 Framed-IPv6-Prefixs	5.3.2.213	O		1,2,3
>>R3 Visited-Framed-IP-Address	5.3.2.362	O		1,2,3
>>R3 Visited-Framed-IPv6-Prefixs	5.3.2.363	O		1,2,3
>>R3 Framed-Interface-Ids	5.3.2.364	O		1,2,3
>>R3 Visited-Framed-Interface-Ids	5.3.2.365	O		1,2,3
>>R3 WiMAX Session ID	5.3.2.214	M		1,2,3
>>R3 Packet Flow Descriptor	5.3.2.215	M		1,2,3
>>>R3 Packet Data Flow ID	5.3.2.216	M		1,2,3
>>>R3 Service Profile ID	5.3.2.218	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Uplink QoS ID	5.3.2.222	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Downlink QoS ID	5.3.2.223	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>SFID	5.3.2.184	M	Associated SFID (one or two).	1,2,3
> REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS/AMS.	1,2,3
>>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.	1,2
>>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.	1,2

TLV	Reference	M/O	Notes	Applicability[4]
>>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.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		
>>Multicast polling group CID support	5.3.2.463	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.	1,2
>>>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.	1,2
>>>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.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

TLV	Reference	M/O	Notes	Applicability[4]
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2

TLV	Reference	M/O	Notes	Applicability[4]
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O		3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O		3
>>Multicarrier capabilities	5.3.2.485	O		3
>>Zone Switch Mode Support	5.3.2.486	O		3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O		3
>>Interference mitigation supported	5.3.2.488	O		3
>>E-MBS capabilities	5.3.2.489	O		3
>>Channel BW and Cyclic prefix	5.3.2.490	O		3
>>frame configuration to support legacy R1.0	5.3.2.491	O		3
>>Persistent Allocation support	5.3.2.492	O		3
>>Group Resource Allocation support	5.3.2.493	O		3
>>Co-located coexistence capability support	5.3.2.494	O		3
>>HO Trigger Metric Support	5.3.2.326	O		3
>>EBB Handover support	5.3.2.495	O		3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O		3
>>Capability for sounding antenna switching support	5.3.2.497	O		3

TLV	Reference	M/O	Notes	Applicability[4]
>>Antenna configuration for sounding antenna switching	5.3.2.498	O		3
>>ROHC support	5.3.2.499	O		3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O		3
> State	5.3.2.355	O	State attribute as received in most recent message from AAA server.	1,2,3
> Anchor MM Context	5.3.2.11	O	Contains FA context for the MS/AMS. 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).	1,2,3
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.	1,2,3
>>MIP4 Info	5.3.2.96	M	Mobility context of the MS/AMS.	1,2,3
>>>HA IP Address	5.3.2.75	M	IP address of the current HA.	1,2,3
>>>Home Address (HoA)	5.3.2.77	M	Home Address (HoA).	1,2,3
>>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA).	1,2,3
>>>Registration Lifetime	5.3.2.147	M	The remaining Mobile IP registration lifetime (measured in seconds).	1,2,3
Context Purpose Indicator	5.3.2.36	M	Bitmap indicating the required context.	1,2,3

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

STEP 19

In Step 3, the EAP phase and PKMv2 SA-TEK or PKMv3 KeyAgreement 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/AMS.

STEP 20

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 4-17:

Table 4-17 – 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/AMS-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 21

The “old” Authenticator, receiving *Relocation_Complete_Req* message with Authentication Result indicating “success”, terminates “reauthentication lock” state and deletes MS/AMS 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 4-18:

Table 4-18 – Relocation_Complete_Rsp Message

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3
PMIP4 Context	5.3.2.373	M		1,2,3
>MIP4 Info	5.3.2.96	M	Mobility context of the MS.	1,2,3
>>HA IP Address	5.3.2.75	O	IP address of the current HA.	1,2,3
>>Home Address (HoA)	5.3.2.77	M	Home Address (HoA).	1,2,3

TLV	Reference	M/O	Notes	Applicability
>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA).	1,2,3
>>Registration Lifetime	5.3.2.147	M	The remaining Mobile IP registration lifetime (measured in seconds).	1,2,3
MS Info	5.3.2.103	O	Contains MS/AMS-related context in the nested IEs.	1,2,3
>MS Authorization Context	5.3.2.100	O	Contains Authorization context parameters of the specific MS/AMS.	1,2,3
>>MSID*	5.3.2.472	CM	Include when MSID privacy is applied.	3
>>MS NAI	5.3.2.105	CM	This TLV SHALL be included if MS Authorization Context is included in the transmitted message.	1,2,3
>>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.	1,2,3
>>R3 WiMAX Capability	5.3.2.207	CM	This TLV SHALL be included if MS Authorization Context is included in the transmitted message.	1,2,3
>>> 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.	1,2,3
>>>R3 Accounting Capabilities	5.3.2.208	CM	This TLV SHALL be included if R3 WiMAX-Capability is included in the transmitted message.	1,2,3
>>>R3 Idle Notification	5.3.2.209	O	This TLV MAY be	1,2,3

TLV	Reference	M/O	Notes	Applicability
Capabilities			included if R3 WiMAX-Capability is included in the transmitted message.	
>>R3 CUI	5.3.2.210	O		1,2,3
>>R3 Class	5.3.2.211	O		1,2,3
>>R3 Framed IP Address	5.3.2.212	O		1,2,3
>>R3 Framed-IPv6-Prefixs	5.3.2.213	O		1,2,3
>>R3 Visited-Framed-IP-Address	5.3.2.362	O		1,2,3
>>R3 Visited-Framed-IPv6-Prefixs	5.3.2.363	O		1,2,3
>>R3 Framed-Interface-Ids	5.3.2.364	O		1,2,3
>>R3 Visited-Framed-Interface-Ids	5.3.2.365	O		1,2,3
>>R3 WiMAX Session ID	5.3.2.214	CM	This TLV SHALL be included if MS Authorization Context is included in the transmitted message.	1,2,3
>>R3 Packet Flow Descriptor	5.3.2.215	CM	This TLV SHALL be included if MS Authorization Context is included in the transmitted message.	1,2,3
>>>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.	1,2,3
>>>R3 Service Profile ID	5.3.2.218	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Uplink QoS ID	5.3.2.222	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Downlink QoS ID	5.3.2.223	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>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.	1,2,3

TLV	Reference	M/O	Notes	Applicability
>REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS.	1,2,3
>>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.	1,2
>>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.	1,2
>>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.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>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.	1,2
>>>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.	1,2
>>>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	1,2

TLV	Reference	M/O	Notes	Applicability
			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.	1,2
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

TLV	Reference	M/O	Notes	Applicability
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O		3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O		3
>>Multicarrier capabilities	5.3.2.485	O		3
>>Zone Switch Mode Support	5.3.2.486	O		3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O		3
>>Interference mitigation supported	5.3.2.488	O		3
>>E-MBS capabilities	5.3.2.489	O		3
>>Channel BW and Cyclic prefix	5.3.2.490	O		3
>>frame configuration to support legacy R1.0	5.3.2.491	O		3
>>Persistent Allocation support	5.3.2.492	O		3
>>Group Resource Allocation support	5.3.2.493	O		3
>>Co-located coexistence capability support	5.3.2.494	O		3
>>HO Trigger Metric Support	5.3.2.326	O		3
>>EBB Handover support	5.3.2.495	O		3

TLV	Reference	M/O	Notes	Applicability
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O		3
>>Capability for sounding antenna switching support	5.3.2.497	O		3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O		3
>>ROHC support	5.3.2.499	O		3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O		3
Accounting Context	5.3.2.204	O	Accounting Context.	1,2,3
>Accounting Mode Provisioning	5.3.2.243	CM	This TLV SHALL be included if Accounting Context is included in the transmitted message.	1,2,3
>>Accounting Type	5.3.2.247	CM	This TLV SHALL be included if Accounting Mode Provisioning is included in the transmitted message.	1,2,3
>> 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.	1,2,3
>>Accounting Number of ToDs	5.3.2.256	O	The number of Time of Day Tariff Switch TLVs.	1,2,3
>>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	1,2,3

TLV	Reference	M/O	Notes	Applicability
			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 message.	1,2,3
>>>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.	1,2,3
>R3 Acct Session Time	5.3.2.361	O	The number of seconds the flow or session was active.	1,2,3
>R3 Active Time	5.3.2.286	O	The number of seconds the session was not in Idle Mode.	1,2,3
Context Purpose Indicator	5.3.2.36	O	Bitmap indicating the required context.	1,2,3
PPAC	5.3.2.65	O	Describes the Prepaid Capabilities of the ASN.	1,2,3
>AvailableInClient	5.3.2.89	CM	This TLV SHALL be included if PPAC is included in the transmitted message.	1,2,3

STEP 22

Table 4-19 – 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.

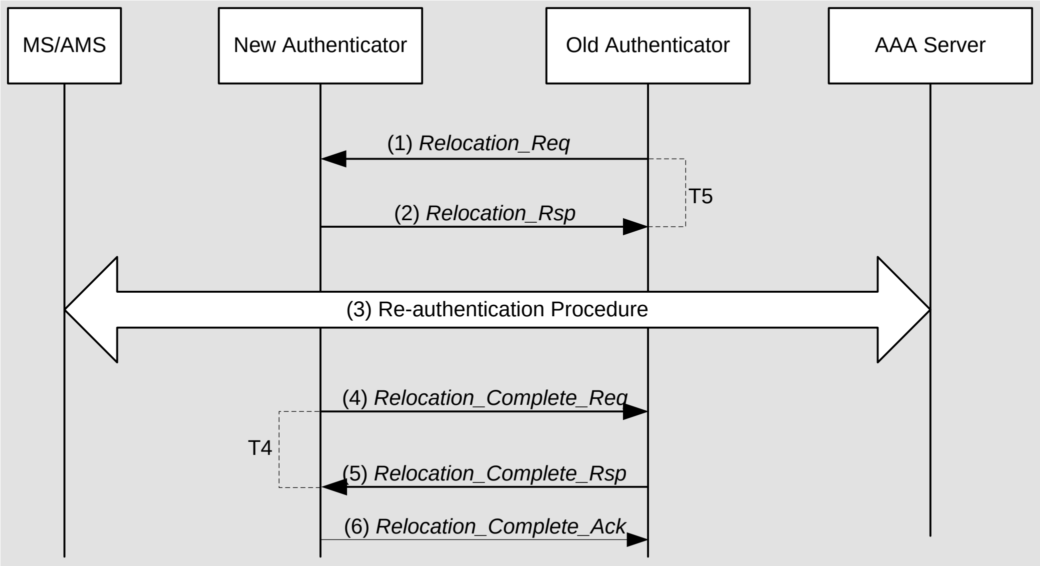

MS/AMS
New Authenticator
Old Authenticator
AAA Server
(1) Relocation_Req
T5
(2) Relocation_Rsp
(3) Re-authentication Procedure
(4) Relocation_Complete_Req
T4
(5) Relocation_Complete_Rsp
(6) Relocation_Complete_Ack

Figure 4-17 – 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 4-20:

Table 4-20 – Relocation_Req from "Old" Authenticator to "New" Authenticator

IE	Reference	M/O	Notes	Applicability
Context Purpose Indicator	5.3.2.36	M		1,2,3
MS Info	5.3.2.103	M	Contains MS/AMS-related context in the nested IEs.	1,2,3
>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.	1,2,3

IE	Reference	M/O	Notes	Applicability
>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.	1,2,3
> MS Security History	5.3.2.108	M	Provides MS/AMS Security history – PMK SN.	1,2,3
>>PMK SN	5.3.2.133	M		1,2,3
>>MS NAI	5.3.2.105	M		1,2,3
>>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.	1,2,3
>>Authorization Policy Support	5.3.2.21	M		1,2,3
>>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.	1,2,3
>> 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.	1,2,3
> MS Authorization Context	5.3.2.100	M	Contains Authorization context parameters of the specific MS/AMS.	1,2,3
>>MSID*	5.3.2.472	CM	Include when MSID privacy is applied.	3
>>MS NAI	5.3.2.105	M		1,2,3

IE	Reference	M/O	Notes	Applicability
>>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.	1,2,3
>>R3 WiMAX Capability	5.3.2.207	M		1,2,3
>>>R3 Accounting Capabilities	5.3.2.208	M		1,2,3
>>> R3 WiMAX-Release	5.3.2.441	M	WiMAX release negotiated during Initial Network Entry.	1,2,3
>>R3 CUI	5.3.2.210	O		1,2,3
>>R3 Class	5.3.2.211	O		1,2,3
>>R3 Framed IP Address	5.3.2.212	O		1,2,3
>>R3 Framed-IPv6-Prefixs	5.3.2.213	O		1,2,3
>>R3 Visited-Framed-IP-Address	5.3.2.362	O		1,2,3
>>R3 Visited-Framed-IPv6-Prefixs	5.3.2.363	O		1,2,3
>>R3 Framed-Interface-Ids	5.3.2.364	O		1,2,3
>>R3 Visited-Framed-Interface-Ids	5.3.2.365	O		1,2,3
>>R3 WiMAX Session ID	5.3.2.214	M		1,2,3
>>R3 Packet Flow Descriptor	5.3.2.215	M		1,2,3
>>>R3 Packet Data Flow ID	5.3.2.216	M		1,2,3
>>>R3 Service Profile ID	5.3.2.218	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Uplink QoS ID	5.3.2.222	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Downlink QoS ID	5.3.2.223	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>SFID	5.3.2.184	M	Associated SFID (one or two).	1,2,3

IE	Reference	M/O	Notes	Applicability
> REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS.	1,2,3
>>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.	1,2
>>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.	1,2
>>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.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>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.	1,2
>>>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.	1,2

IE	Reference	M/O	Notes	Applicability
>>>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.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2

IE	Reference	M/O	Notes	Applicability
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
> Authenticator ID	5.3.2.19	O	Indicates the ID of the ‘old’ Authenticator GW.	1,2,3
> State	5.3.2.355	O	State attribute as received in most recent message from AAA server.	1,2,3
> Anchor MM Context	5.3.2.11	O	Contains FA Context for the MS/AMS, If included it indicates the suggestion for FA relocation.	1,2,3
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.	1,2,3
>>MIP4 Info	5.3.2.96	M	Mobility context of the MS/AMS.	1,2,3
>>>HA IP Address	5.3.2.75	M	IP address of the current HA.	1,2,3
>>>Home Address (HoA)	5.3.2.77	M	Home Address (HoA).	1,2,3
>>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA).	1,2,3

IE	Reference	M/O	Notes	Applicability
>>>Registration Lifetime	5.3.2.147	M	The remaining Mobile IP registration lifetime (measured in seconds).	1,2,3
BS Info	5.3.2.26	O	Contains relevant Serving BS/ABS context in the nested IEs.	1,2,3
> BS ID	5.3.2.25	CM	Serving BS ID.	1,2,3

STEP 2

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

Table 4-21 – 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/AMS 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.

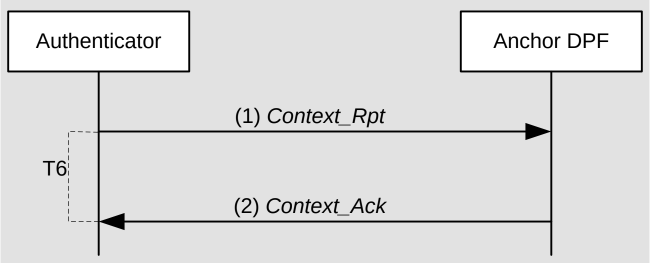


Figure 4-18 – Authenticator Update Notification Procedure

STEP 4

The “new” Authenticator updates the MS/AMS Anchor DP with the “new” MS/AMS Anchor Authenticator location using *Context_Rpt* message. The composition of this *Context_Rpt* message is presented in Table 4-22:

Table 4-22 – 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[5]	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)

[5] 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.

IE	Reference	M/O	Notes
>FA-HA Key Lifetime	5.3.2.67	O	Time of FA-HA key remaining valid. (in case of CMIP only)

STEP 23

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

Table 4-23 – 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/AMS as long as the "currently active" MSK and security context are valid.

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/ABS and is stopped upon receiving the corresponding Key_Change_Ack.
- T2: is started by the BS/ABS 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.
- $T_{Relo\_Comp\_Rsp}$: 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 4-24 defines the default timer values and also indicates the range of the recommended duration of these timers.

Table 4-24 – Timers and Timing Considerations

Timers	Default Values (msec)	Maximum Timer Value (msec)
T_1	TBD	TBD
T_2	TBD	TBD
T_3	TBD	TBD
T_4	TBD	TBD
T_5	TBD	TBD
T_6	TBD	TBD
$T_{Relo\_Comp\_Rsp}$	TBD	TBD

4.4.1.5.6.2 Error Handling Scenarios

Table 4-25 defines the lists the various error conditions during Re-authentication.

Table 4-25 – Error Handling Scenarios

Error Condition	Failure Case	Action
1	Authenticator receives the RADIUS Access-Reject or the Diameter WDEA with EAP Failure indication	Authenticator SHALL initiate the MS/AMS Network exit.
2	Incomplete Reauthentication process such as due to failed transport	MS/AMS current session SHALL NOT be terminated as long as the “currently active” MSK and security context are valid.
3	BS/ABS detects PKMv2/PKMv3 3-way hand shake failure	BS/ABS sends Key_Change_Cnf message with Key Change Indicator TLV set to indicate “failure”. MS/AMS 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 4-26 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 4-26.

Table 4-26 – 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/ABS	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).
$T_{Relo\_Comp\_Rsp}$	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 (IPv4, IPv6, or dual IPv4/IPv6), CMIP (IPv4, IPv6, or dual IPv4/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: DHCP mode (relay or proxy), MIP mode (Simple IPv4, Simple IPv6, CMIPv4, PMIPv4, CMIPv6, PMIPv6), Ethernet services (if provided). 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/AMS at the point when MS/AMS 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/AMS the network service request, and will assign the appropriate network service support for this MS/AMS.

Unless otherwise specified, for feature specific handover, the capability that is negotiated between the HCSN and the ASN-GW is committed to be delivered for this session by the NAP. If the ASN-GW reports a capability that the HCSN selects to use, then that capability SHALL be continued to be provided for the entire WiMAX session. Therefore, handover procedures SHALL take into account the features negotiated during initial network entry for the session in determining whether the session can handover to another ASN-GW or base station. Since the capability is committed to be delivered, the target ASN-GW SHALL reject the HO attempt if the capability is not supported. In this case, the serving ASN-GW can either select another target ASN-GW, keep the session (not handoff to another ASN-GW if possible), or terminate the session.

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/AMS. 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-Capability VSA, the NAS SHALL store this information locally and make it available to be used later for Simple IPv6 service.

If NAS receives either vHA-IP-MIP4 or hHA-IP-MIP4 attributes in RADIUS Access-Accept packet or Diameter WDEA command, the NAS SHALL store these HAv4 attributes locally and make it available to be used later for either CMIP4 or PMIP4 services to the MS/AMS.

If NAS receives either vHA-IP-MIP6 and/or hHA-IP-MIP6 attributes in RADIUS Access-Accept packet or Diameter WDEA command, the NAS SHALL store these HAv6 attributes locally and make it available to be used later for CMIP6 services to the MS/AMS.

If NAS receives either vLMA-IPv6-PMIP6 and/or hLMA-IPv6-PMIP6 attributes in RADIUS Access-Accept message or Diameter WDEA command the NAS SHALL store these PMIP6 attributes locally and make available later for PMIP6 service, if assigned to the MS/AMS. The NAS SHALL also process and store PMIP6 protocol feature authorization hints provided in the PMIP6-Service-Info attribute. If NAS has indicated IPv4 R3 transport capability to the HAAA, the vLMA-IPv4-PMIP6 and/or hLMA-IPv4-PMIP6 attributes in RADIUS Access-Accept or Diameter WDEA SHALL be processed and stored.

If NAS receives Simple ETH Service authorization through the Authorized Network Service 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 Ethernet service.

If NAS receives MIP based ETH Service authorization through the Authorized Network Service attribute and Bootstrapping Mobility Service attribute of WiMAX-Capability VSA, i.e., either vHA-IP-MIP4 or hHA-IP-MIP4 attributes, in RADIUS Access-Accept or Diameter WDEA command, the NAS SHALL store these attributes locally and make it available to be used later for MIP based Ethernet services to the MS/AMS.

If NAS receives either Simple ETH Service authorization or MIP based ETH Service authorization through the Authorized Network Service attribute in the WiMAX-Capability VSA in the RADIUS Access-Accept packet or Diameter WDEA command, the NAS SHALL discard the presence of the vDHCP Server or hDHCP Server attributes in the RADIUS Access-Accept or Diameter WDEA commands and SHALL provide the state of the L2 DHCP Relay authorization locally, to indicate whether the L2 DHCP Relay functionality should be enabled for this MS/AMS.

If NAS receives either vDHCP or hDHCP Server attributes in RADIUS Access-Accept packet or Diameter WDEA command, the NAS SHALL store these attributes locally and make it available to be used in DHCP signaling transaction later. It also indicates that DHCP Relay functionality should be enabled for this MS/AMS.

If NAS does not receive DHCP Server attributes in RADIUS Access-Accept packet or Diameter WDEA command, it indicates that DHCP Proxy functionality should be enabled for this MS/AMS. The NAS SHALL store the IP and Host configuration attributes locally and make them available to be used in DHCP signaling transaction later. It also indicates that DHCP proxy functionality should be enabled for this MS/AMS.

4.4.1.6.2 VCSN Requirement for Network Service Capability Negotiation

If VCSN AAA proxy receives the RADIUS Access-Request packet or Diameter WDER command from the NAS in ASN, the VCSN SHALL attach its own VCSN Network Service Capability attribute to the original RADIUS Access-Request packet or Diameter WDER command sent from ASN and forward this message to HAAA in HCSN.

VCSN SHALL attach vHA and/or vDHCP(v4 and/or v6) Server address to the RADIUS Access-Request packet or Diameter WDER message and forward to HAAA in HCSN if VCSN is capable of providing these services.

VCSN SHALL NOT provide a network Service that it is not authorized for in the RADIUS Access-Accept or Diameter WDEA command indicating successful authentication.

If the VCSN supports PMIP6 mobility management, the VAAA MAY append the LMA capability in the RADIUS Access-Request's VCSN Network Service Capability indication. In that case the IPv6 address of the LMA in the VCSN SHALL be present.

HAAA in HCSN SHALL send a RADIUS Access-Reject packet or Diameter WDEA command indicating failure to 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/AMS based on received ASN Network Service Capability, MS/AMS 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/AMS 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/AMS 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/AMS 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 NAS doesn't indicate R3 transport IPv4 capability, HAAA SHALL not include h/vLMA-IPv4-PMIP6 in the RADIUS Access-Accept packet or Diameter WDEA command.

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/ABS (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/PKMv3 EAP-related messages in IEEE 802.16e/m. 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 4-27 – List of Authentication Relay Protocol Messages

AR_EAP_Start
AR_EAP_Transfer

The Base Station acts as an EAP Relay entity. It transfers an EAP message received from the MS/AMS over R1 to the Authenticator and vice versa. For each valid EAP message that the Base Station receives over PKMv2/v3 messages, it sends a corresponding AuthRelay message to Authenticator (including the received EAP message as a payload). The BS/ABS processes only valid PKMv2/v3 EAP-related MAC messages on the air interface and discards non-valid PKMv2/v3 EAP-related messages (e.g., unprotected PKMv2 EAP-Start, unprotected PKMv3 Reauth-Request, unprotected PKMv2/v3 EAP-Transfer during re-authentication, protected PKMv2/v3 messages which BS/ABS fails to validate, etc.).

The AuthRelay messages represented by different Message Types correspond one-to-one to the PKMv2/PKMv3 EAP-related messages on 802.16e/m interface. The mapping between PKMv2/v3 and AuthRelay messages is presented in Table 4-28.

Table 4-28 – Authentication Relay Messages Mapping to PKMv2/v3 and Vice Versa

AuthRelay Message	PKMv2/v3 message code	PKMv2/v3 REQ/ RSP	Notes
AR_EAP_Start	EAP-Start or PKMv3 Reauth-Request	REQ	PKMv2 EAP-Start or PKMv3 Reauth-Request is sent by MS/AMS to initiate EAP reauthentication. *AR_EAP_Start* is sent by the BS/ABS to the Authenticator. If PKMv2 EAP-Start or PKMv3 Reauth-Request is not protected by CMAC, the BS drops this message and does not send an *AR_EAP_Start* to the Authenticator PKMv2/v3: MS/AMS → BS/ABS AuthRelay: BS/ABS → Authenticator
AR_EAP_Transfer	EAP-Transfer	REQ	This message is used to exchange EAP payload between peers. PKMv2/v3: MS/AMS→ BS/ABS AuthRelay: BS/ABS → Authenticator
		RSP	AuthRelay: Authenticator → BS/ABS PKMv2/v3: BS/ABS→ MS/AMS

Note: AuthRelay messages are not formatted as PKMv2/v3 messages – e.g., does not include CMAC TLV, PKM Identifier field, etc. that are created in BS/ABS.

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/ABS 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 4-19 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.

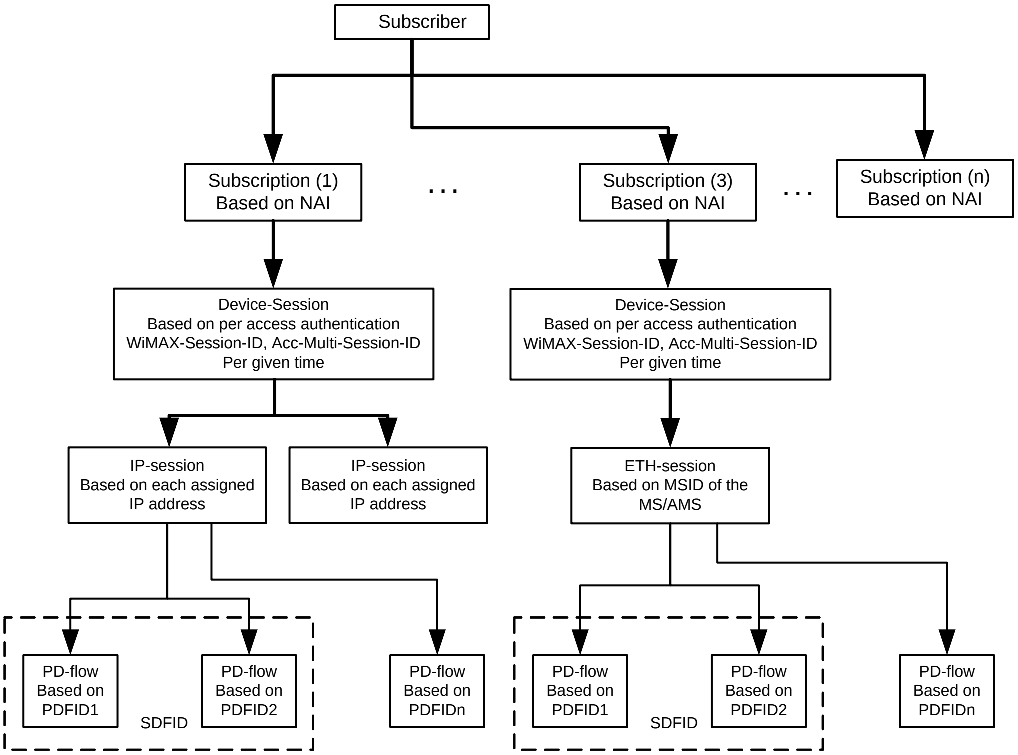

Subscriber
Subscription (1) Based on NAI
. . .
Subscription (3) Based on NAI
. . .
Subscription (n) Based on NAI
Device-Session Based on per access authentication WiMAX-Session-ID, Acc-Multi-Session-ID Per given time
Device-Session Based on per access authentication WiMAX-Session-ID, Acc-Multi-Session-ID Per given time
IP-session Based on each assigned IP address
IP-session Based on each assigned IP address
ETH-session Based on MSID of the MS/AMS
PD-flow Based on PDFID1
PD-flow Based on PDFID2
SDFID
PD-flow Based on PDFIDn
PD-flow Based on PDFID1
PD-flow Based on PDFID2
SDFID
PD-flow Based on PDFIDn

Figure 4-19 – 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 4-29 – 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 4-30. 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 4-30 – Accounting Modes

Accounting Mode	Description	ID
Session	For IP Service: 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. For Eth Service: One to one mapping between ETH-sessions and device-session. ETH-session is based on MSID of the MS/AMS.	For IP Service: IP address assigned to the MS/AMS. For ETH Service: MSID of the MS/AMS
PD-flow	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 is bound to a single WiMAX service flow (or two if the packet data flow is bi-directional). Several PD-flows can be grouped by a service data flow, identified by an SDFID.	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/AMS. 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.

[98] 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 5.4.3 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 PPS indicating support for On-line accounting at the ASN and or the HA. If the Subscription Session requires on-line charging the PPS assigns a prepaid accounting quota (PPAQ) to the PPC using RADIUS Access-Accept packets.

As the session continues, the PPC and the PPS replenish the quotas by exchanging RADIUS packets. A typical online interaction is illustrated in Figure 4-20.

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

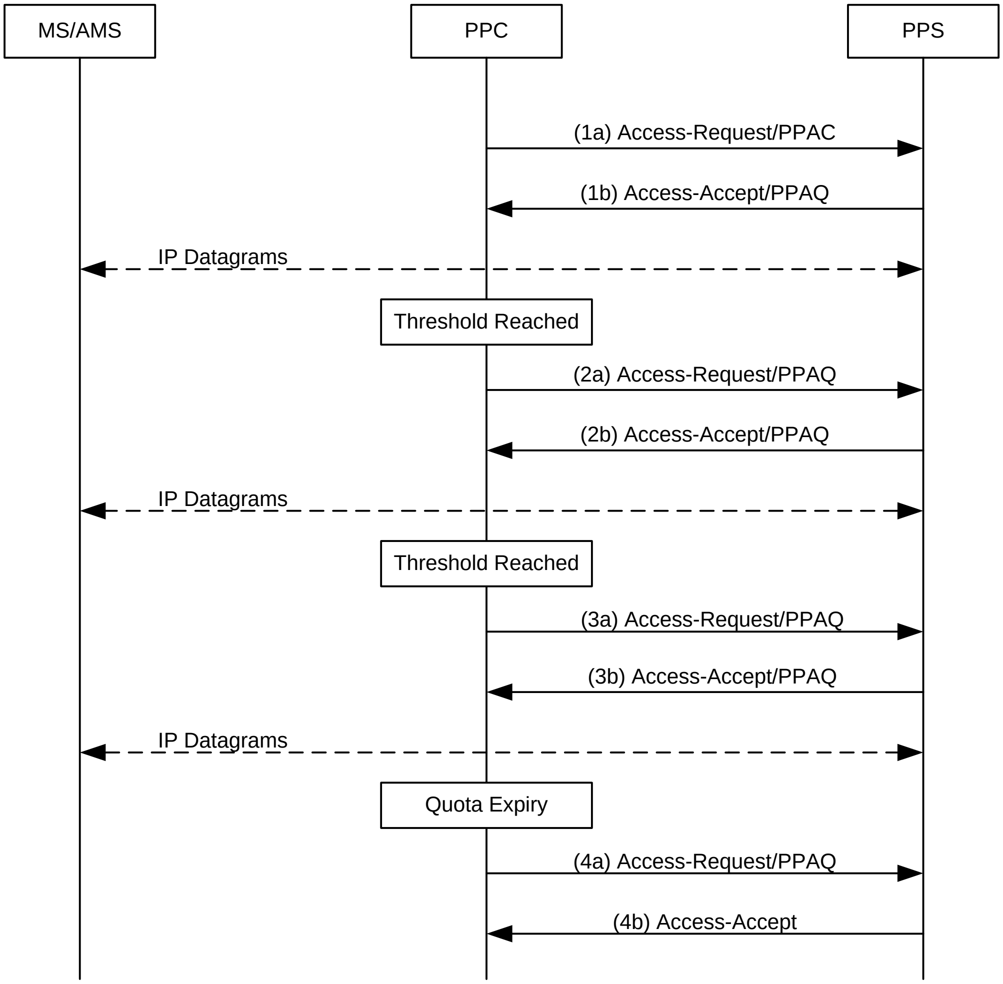


Figure 4-20 – Online Accounting Procedures

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 5.4.3 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 5.4.3.

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) [64]; in addition, Ro interface definition in [100] is also taken as an input, including its simplifications of, and enhancements to RFC4006 [64]. 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 [64].

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/AMS. 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

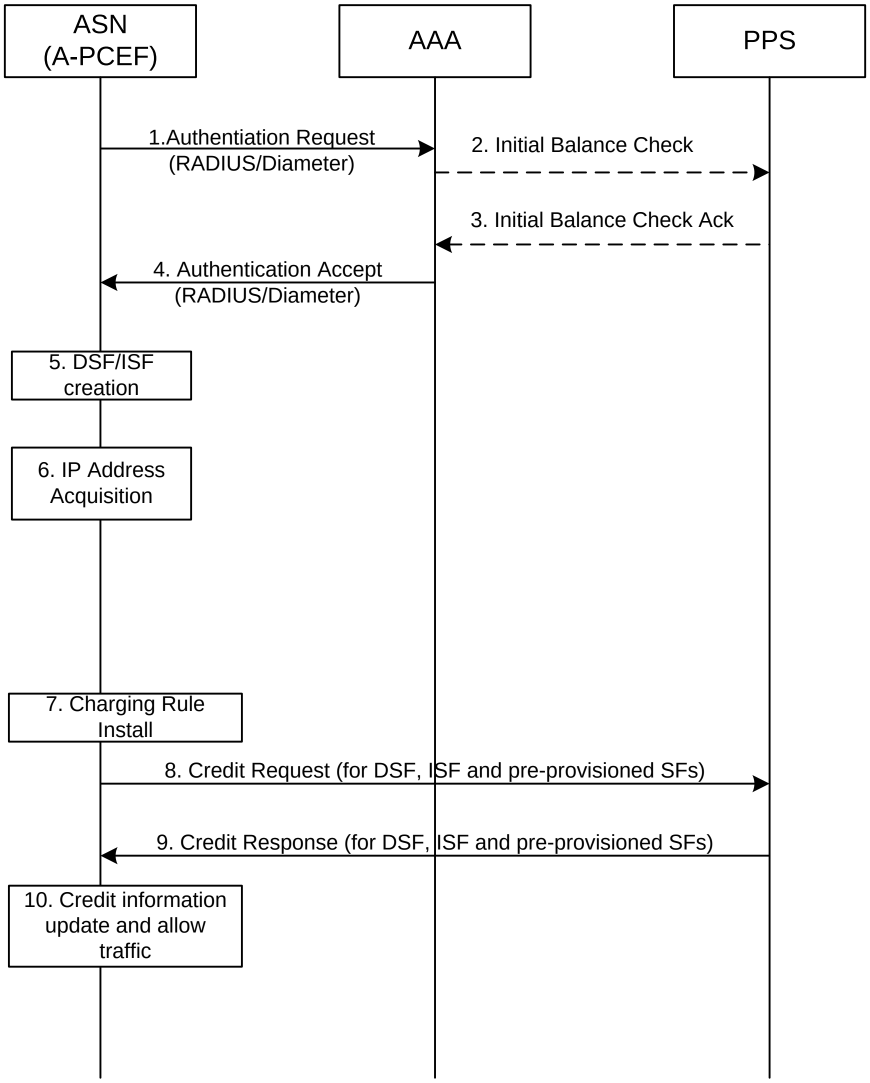

ASN
(A-PCEF)
AAA
PPS
1.Authentiation Request
(RADIUS/Diameter)
2. Initial Balance Check
3. Initial Balance Check Ack
4. Authentication Accept
(RADIUS/Diameter)
5. DSF/ISF creation
6. IP Address Acquisition
7. Charging Rule Install
8. Credit Request (for DSF, ISF and pre-provisioned SFs)
9. Credit Response (for DSF, ISF and pre-provisioned SFs)
10. Credit information update and allow traffic

Figure 4-21 depicts the message flows for initial and pre-provisioned service flow creation.

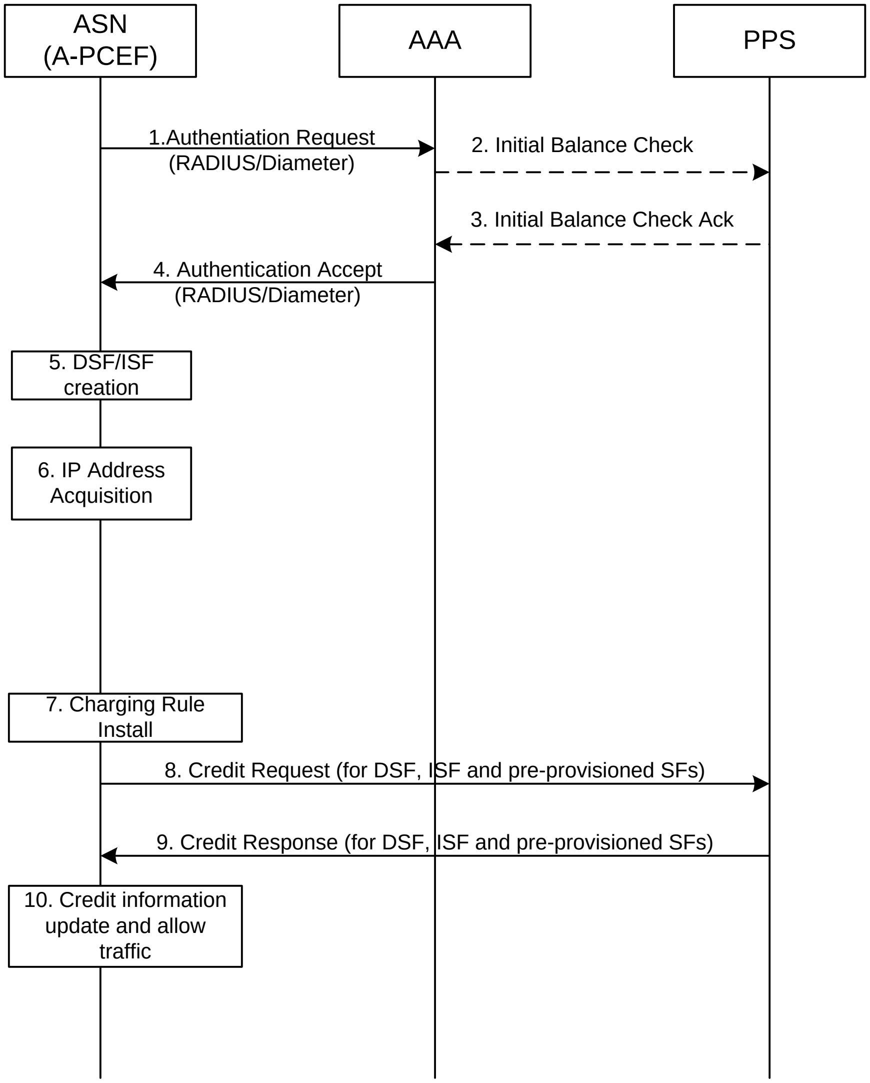

ASN (A-PCEF)
AAA
PPS
1.Authentiation Request (RADIUS/Diameter)
2. Initial Balance Check
3. Initial Balance Check Ack
4. Authentication Accept (RADIUS/Diameter)
5. DSF/ISF creation
6. IP Address Acquisition
7. Charging Rule Install
8. Credit Request (for DSF, ISF and pre-provisioned SFs)
9. Credit Response (for DSF, ISF and pre-provisioned SFs)
10. Credit information update and allow traffic

Figure 4-21 – 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 responses to the authentication request received in step 1 from the ASN and includes an indication that online accounting is required.

5. DSF and ISF are created and resources are allocated to the MS/AMS. Optionally, pre-provisioned SFs could be created but traffic SHALL be blocked until PCRF authorizes traffic and PPS provides sufficient quota for the DSF/ISF/PPSF (see step 10).

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, DSF 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 4-22 depicts the message flows for MS/AMS/SS/BS/ABS initiated session termination:

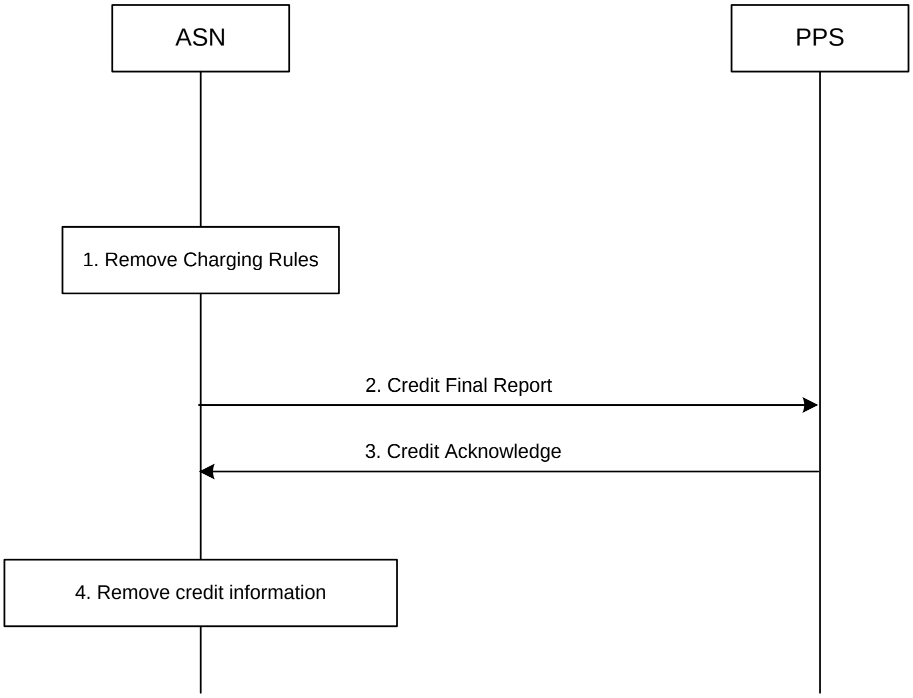


Figure 4-22 –Session Termination

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

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

a. The BS/ABS, 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/ABS is optional and is specified in Section 5.3.2.373. If the BS/ABS 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 DSF/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 [52].

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 Local Routing Accounting

There are two Service-Ids (in RADIUS) or Service-Context-Ids (in DIAMETER) for a local routing enabled service, respectively addressing the local-routed traffic and normal traffic of it. An ALR tag is used to distinguish the "local-routed" Service-Id (in RADIUS) or Service-Context-Id (in DIAMETER) from the "normal" one, i.e. the local-routed one has an ALR tag in it while the normal one has no ALR tag.

For RADIUS, when a given service is local routing enabled, in addition to the normal PPAQ with normal Service-Id, the PPC sends an additional PPAQ identified by a Service-ID with ALR tag to PPS to indicate the service is local routing enabled and requests quota for local-routed traffic. Upon receiving a PPAQ with Service-Id with ALR tag, the PPS regards the service as local routing enabled and assigns individual PPAQs to the normal and local-routed traffic of it. The two PPAQs are identified by a normal Service-Id and a local-routed Service-Id respectively.

For DIAMETER, when a given service is local routing enabled, in addition to the normal CCR with normal Service-Context-Id, the PPC sends an additional CCR identified by a Service-Context-Id with ALR tag to PPS to indicate the service is local routing enabled and requests quota for local-routed traffic. Upon receiving a CCR with Service-Context-Id with ALR tag, the PPS regards the service as local routing enabled and assigns individual CCRs to the normal and local-routed traffic of it. The two CCRs are identified by a normal Service-Context-Id and a local-routed Service-Context-Id respectively.

4.4.3.3.6 PPC Relocation in case of RADIUS based Online Accounting

Prepaid Client (PPC) is collocated with MS/AMS 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.

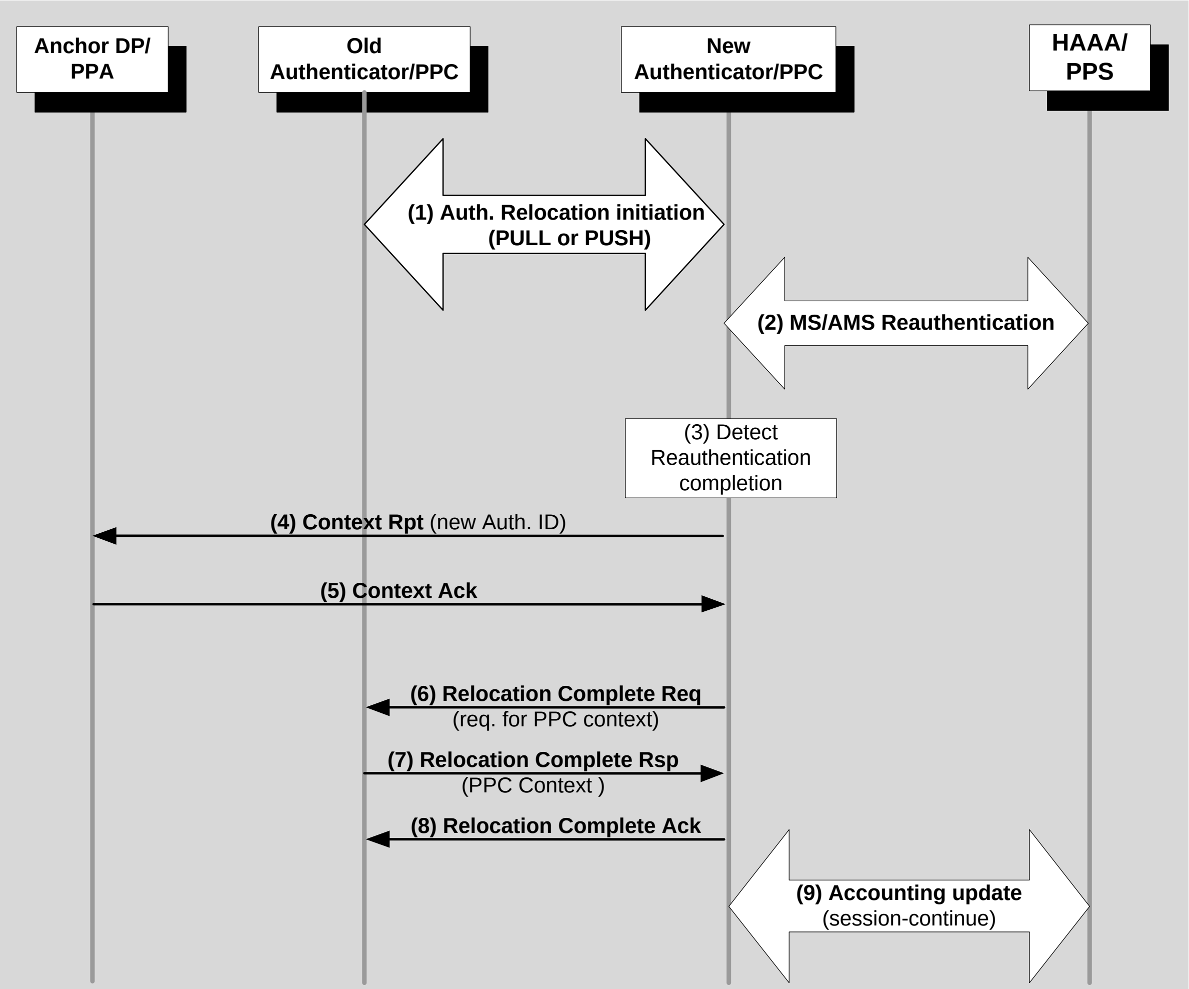

Anchor DP/ PPA
Old Authenticator/PPC
New Authenticator/PPC
HAAA/ PPS
(1) Auth. Relocation initiation (PULL or PUSH)
(2) MS/AMS Reauthentication
(3) Detect Reauthentication completion
(4) Context Rpt (new Auth. ID)
(5) Context Ack
(6) Relocation Complete Req (req. for PPC context)
(7) Relocation Complete Rsp (PPC Context)
(8) Relocation Complete Ack
(9) Accounting update (session-continue)

Figure 4-23 – 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/AMS Reauthentication occurs in the "new" Authenticator entity. This includes EAP Phase and PKMv2/PKMv3 3WHS Phase.

STEP 3

In the case the "new" Authenticator detects successful completion of reauthentication process (successful completion of PKMv2/PKMv3 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_R*sp 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).

4.4.3.3.7 PPC Relocation in case of Diameter based Online Accounting

Figure 4-24 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].

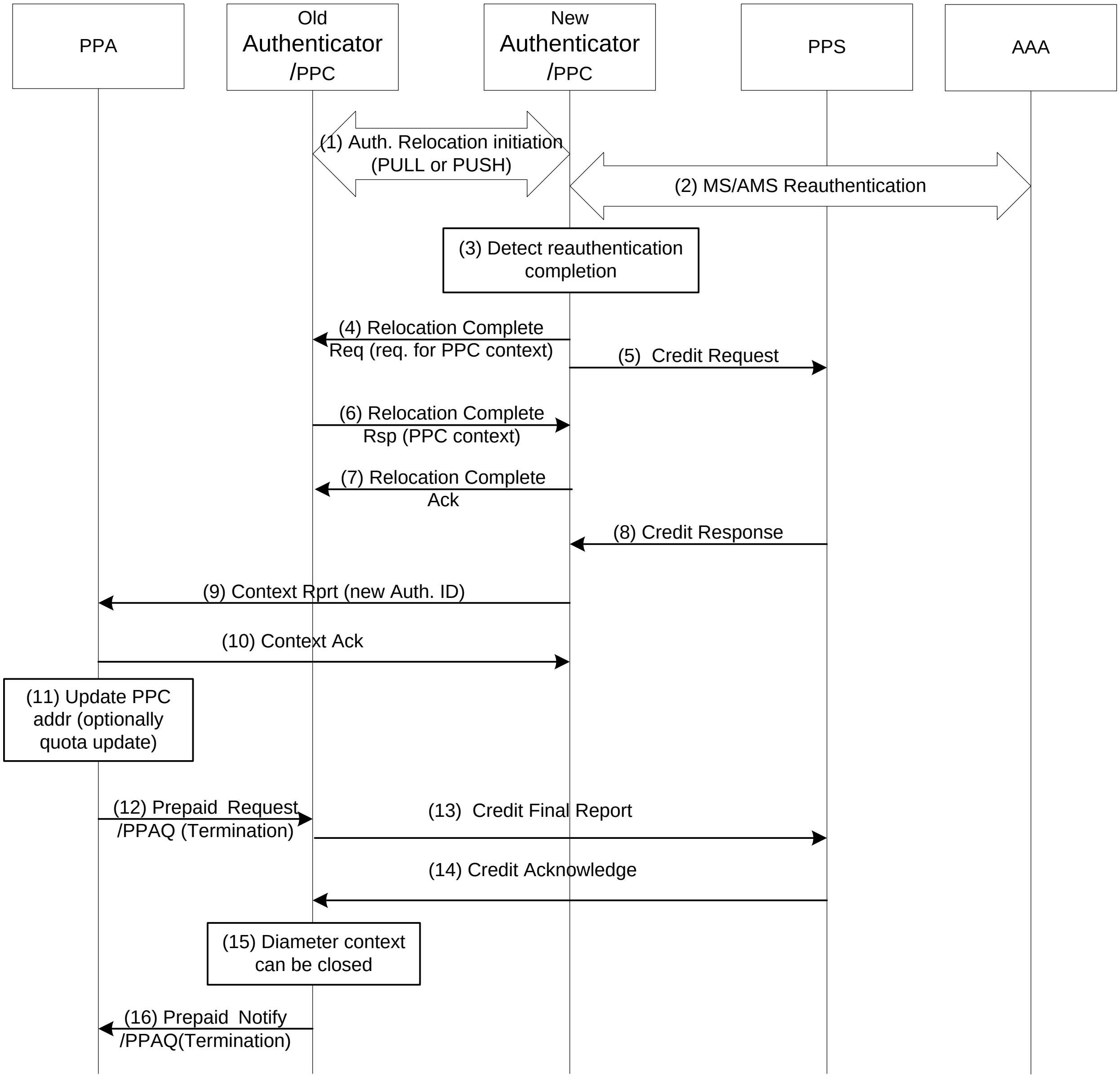

PPA
Old Authenticator /PPC
New Authenticator /PPC
PPS
AAA
(1) Auth. Relocation initiation (PULL or PUSH)
(2) MS/AMS Reauthentication
(3) Detect reauthentication completion
(4) Relocation Complete Req (req. for PPC context)
(5) Credit Request
(6) Relocation Complete Rsp (PPC context)
(7) Relocation Complete Ack
(8) Credit Response
(9) Context Rprt (new Auth. ID)
(10) Context Ack
(11) Update PPC addr (optionally quota update)
(12) Prepaid Request /PPAQ (Termination)
(13) Credit Final Report
(14) Credit Acknowledge
(15) Diameter context can be closed
(16) Prepaid Notify /PPAQ(Termination)

Figure 4-24 – 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/PKMv3 3WHS Phase.

STEP 3

In the case the “new” Authenticator detects successful completion of re-authentication process (successful completion of PKMv2/PKMv3 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.

4.4.3.3.8 PPA Relocation

Prepaid Agent (PPA) is collocated with MS/AMS Anchor DPF/ FA functional entities. When Anchor DPF/ FA relocation scenario occurs, PPA is also relocated. The PMIP4 scenario is presented in the section [4.8.2.3.8]. The CMIP4 scenario is described in [4.8.3.3]. Anchor DPF/FA Relocation also accompanies HLD Relocation, if HLD is co-located 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.

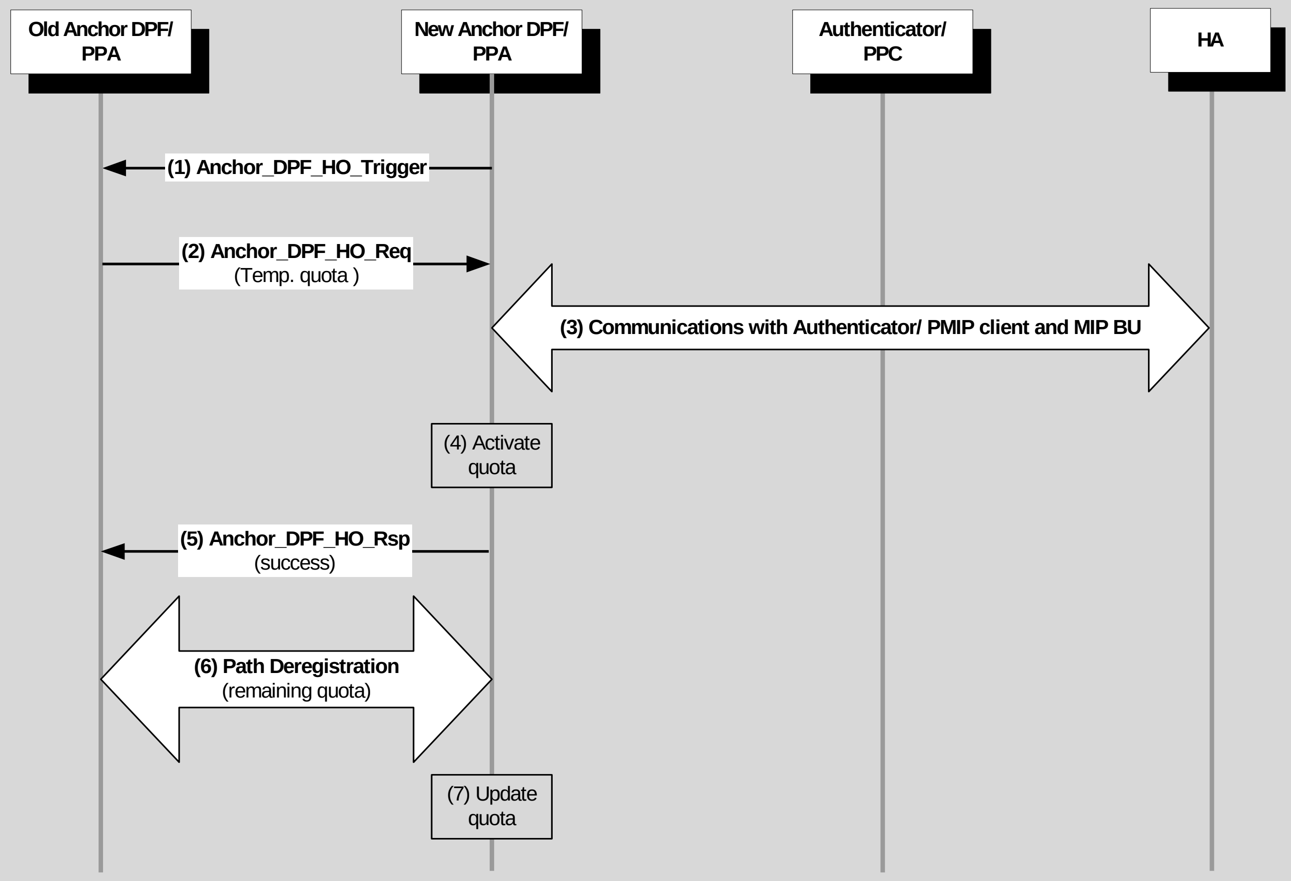


Figure 4-25 – PPA Relocation

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 4-144.

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.

4.4.3.3.9 PPA-PPC quota(s) update

PPA communicates online accounting events with PPC (quota updates/ requests) using *Prepaid_Request* and *Prepaid Notify* messages.

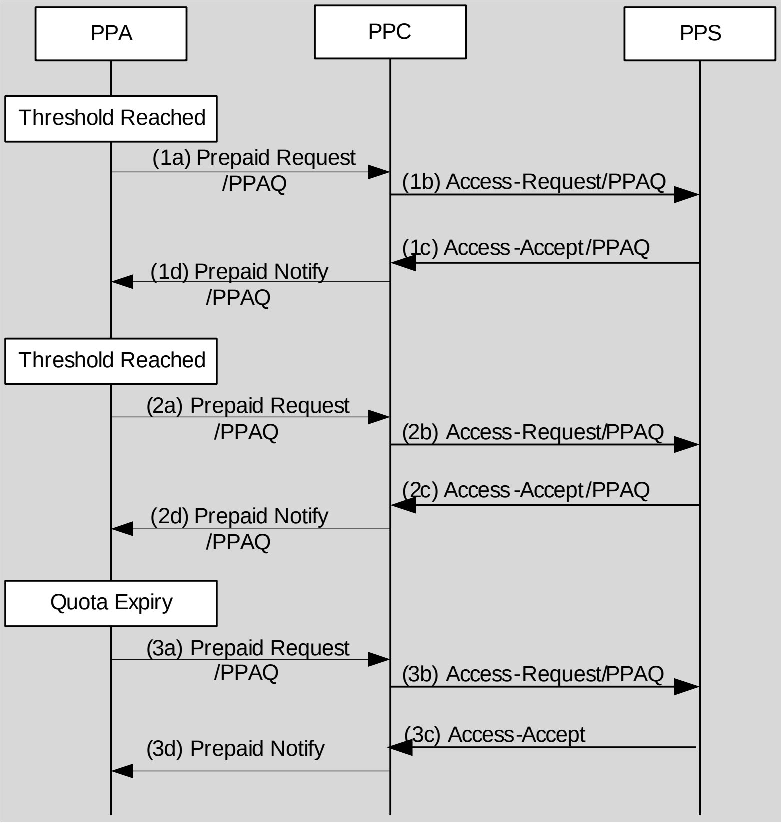


Figure 4-26 – PPA-PPC quota(s) update

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 4-19.

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/ABS. 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/ABS, the accounting agent may report byte counts for the dropped frame over the air.

As the MS/AMS moves around and changes the BS/ABS, 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 4-27.

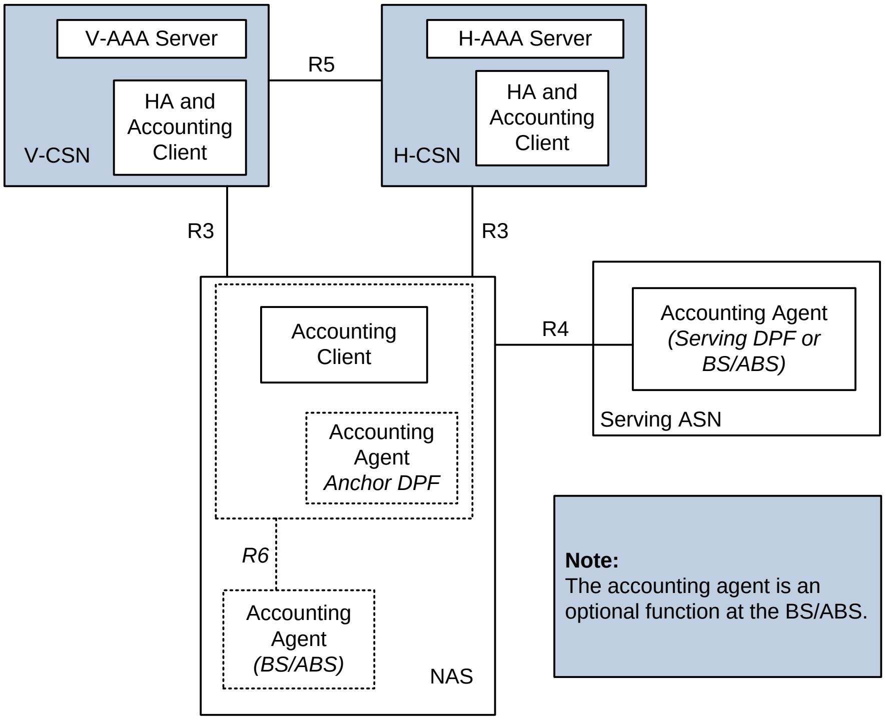

V-AAA Server
HA and Accounting Client
V-CSN
R5
H-AAA Server
HA and Accounting Client
H-CSN
R3
R3
Accounting Client
Accounting Agent Anchor DPF
R4
Accounting Agent (Serving DPF or BS/ABS)
Serving ASN
R6
Accounting Agent (BS/ABS)
NAS
Note:
The accounting agent is an optional function at the BS/ABS.

Figure 4-27 – Accounting Client and Agent

An accounting session is delineated by an Accounting-Request-Start and an Accounting-Request-Stop as per [38] 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 DSF/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-Ssession-Id assigned at network access.

Accounting procedures per accounting session are illustrated in Figure 4-28 in case of RADIUS. For Diameter, the same flow with the corresponding messages takes place.

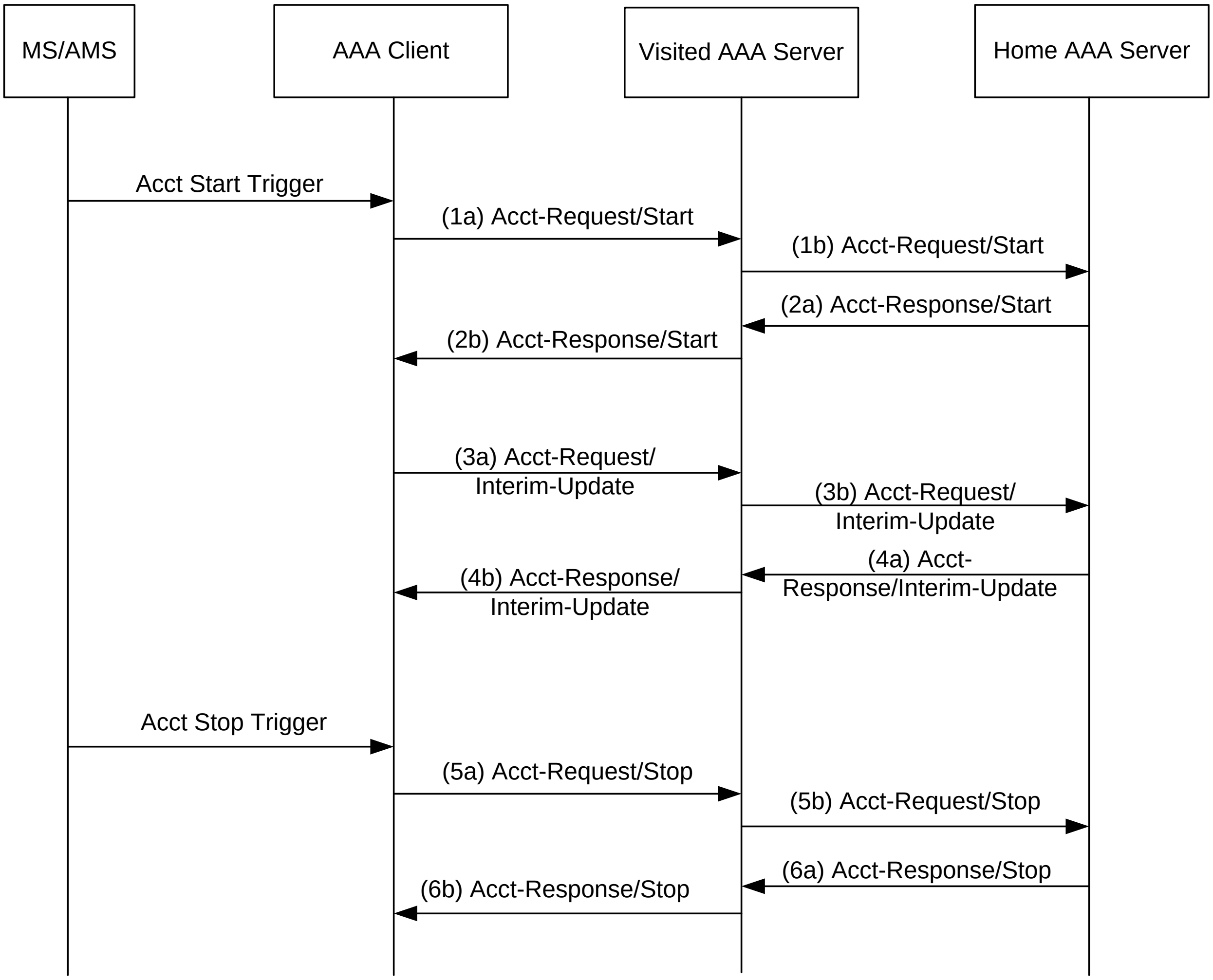


Figure 4-28 – Offline Accounting Procedures

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 2.0 is based on RADIUS Accounting as specified by [41] and [39] and [55] 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) [41] 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 4-31.

Table 4-31 – 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 [39].

In the case of Diameter three modes of operations are supported as defined by the Accounting-Realtime-Required AVP [55]. 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 uses parameter as specified in section 5.3.2.360.
- 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 [39] and [41] as well as to [55] in case of Diameter. The payload of the record is defined by WiMAX and is divided into logical blocks as follows.

Table 4-32 – 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 identity the time the accounting took place. The time zone is also conveyed.
L3 Counters	The attributes in this section report the various L3 counters.
OTA Counters	The attributes in this section report the various over-the-air counters.
Flowspec	The attributes in this section report the flow specification.
QoS	The attributes in this section report the QoS assigned to the flow.

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 5.4.1.6.

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/AMS. 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/AMS.

4.4.3.4.4.2 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 4-29 illustrates the correlation hierarchy and the correlation identifiers associated with each level of correlation.

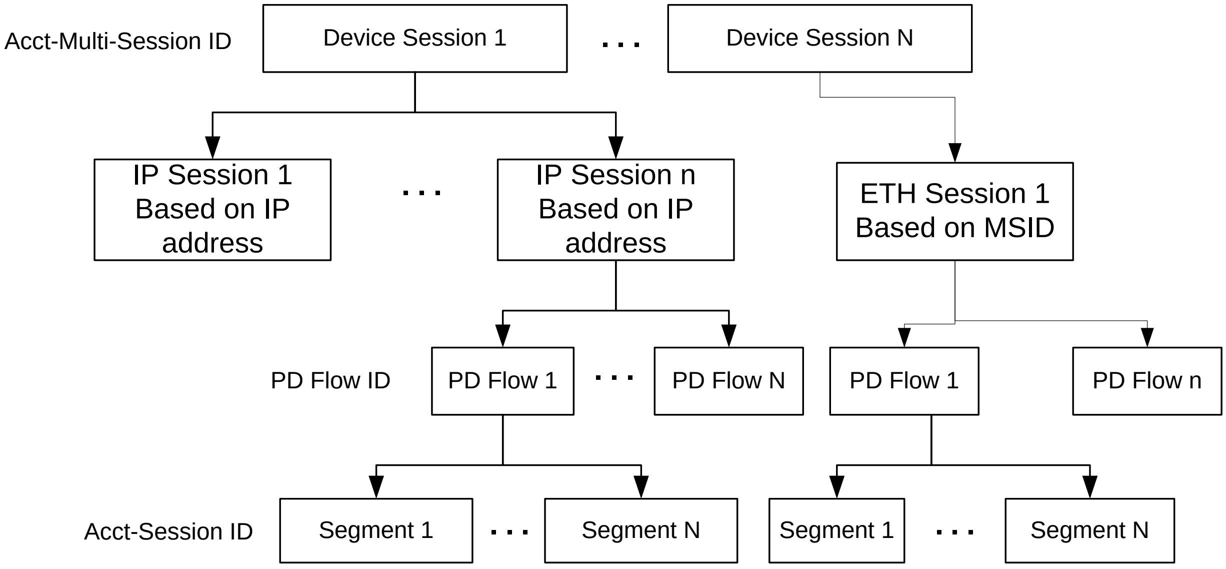


Figure 4-29 – Correlation Hierarchy

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/AMS. 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/AMS. 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/DCR Mode Notification

The anchor authenticator knows when an MS/AMS 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/AMS enters or exits the idle mode. The accounting client at the ASN need not send an accounting interim update message while the MS/AMS 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 Offline (Post-Paid) accounting for Local Routing

When the accounting client (or agent) sends an accounting start message to the accounting server, a VSA/AVP named Local-Routing-Indication may be present in the message to indicate whether the service is local routing enabled or not. If the service is local routing enabled, the accounting client (or agent) co-located with the ASN-GW which performs local routing will record the information of normal traffic and local-routed traffic respectively. The corresponding UDR(s) is (are) generated per the recorded information by the ALR enabled ASN-GW and sent to the accounting server for local routing accounting in the following accounting message(s).

Note: Local routing accounting described here does not apply to HA generated UDR.

4.4.3.4.6 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/ABS 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.

4.4.3.4.7 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.

4.4.3.4.7.1 Bulk Interim Update

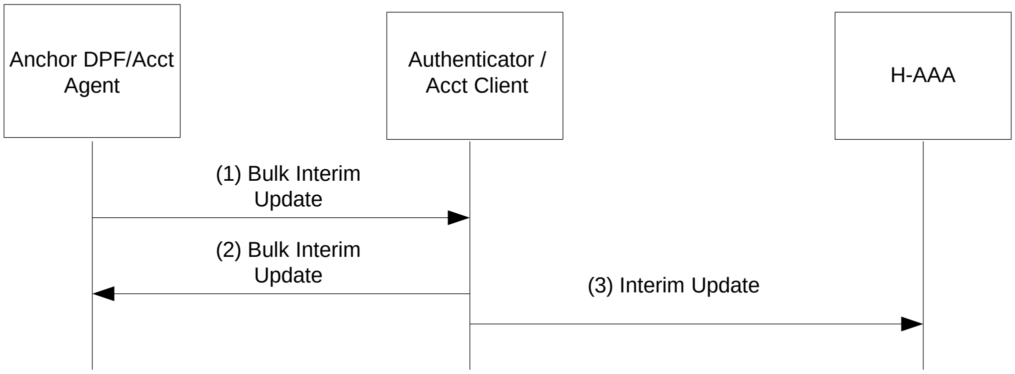


Figure 4-30 – Bulk Interim Update Procedure

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.

4.4.3.4.7.2 Hot-Lining

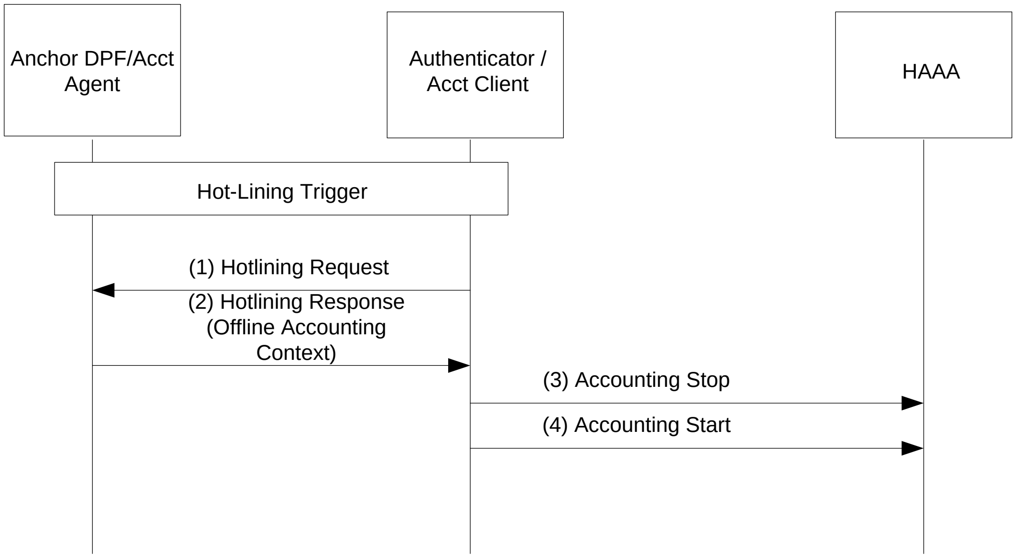


Figure 4-31 – Hot-Lining

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.

4.4.3.4.7.3 Idle Mode Entry

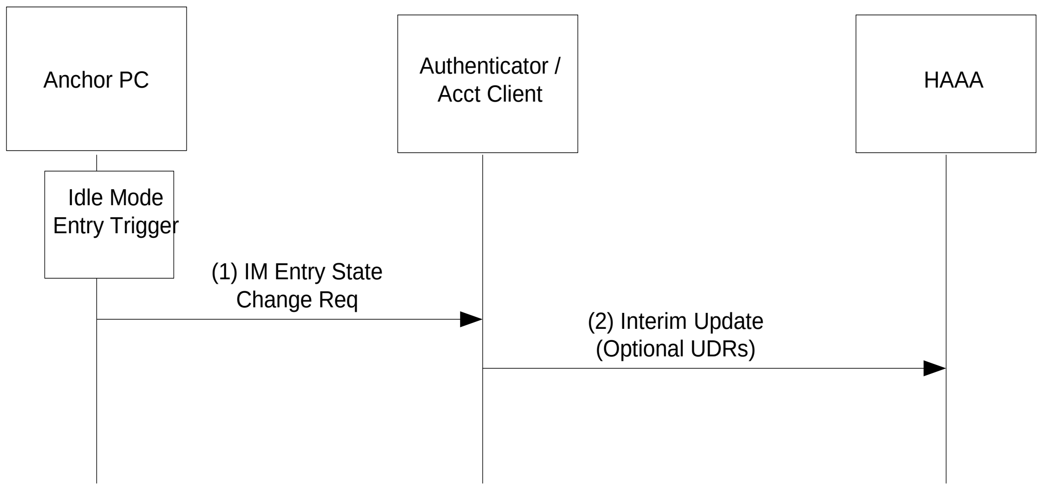

Anchor PC
Authenticator / Acct Client
HAAA
Idle Mode Entry Trigger
(1) IM Entry State Change Req
(2) Interim Update (Optional UDRs)

Figure 4-32 – 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.

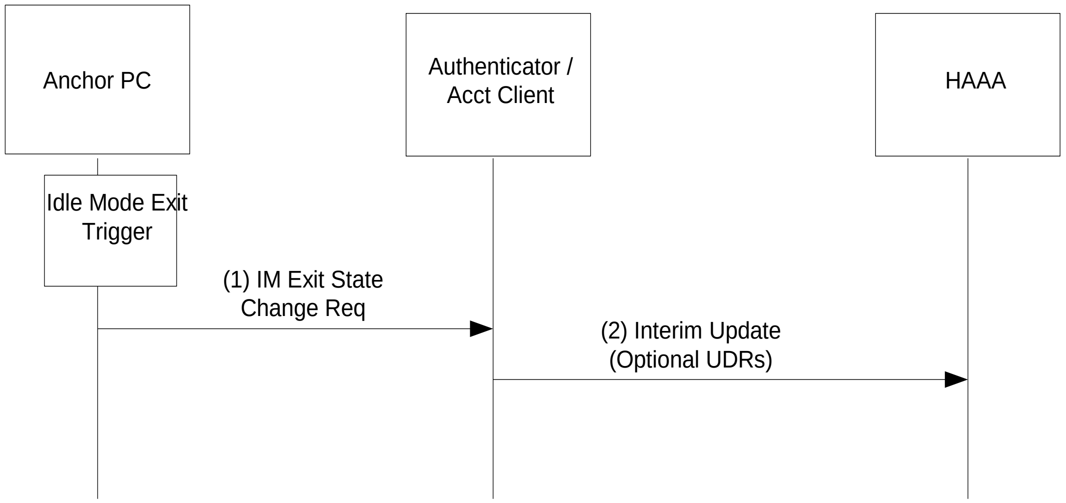

Anchor PC
Authenticator / Acct Client
HAAA
Idle Mode Exit Trigger
(1) IM Exit State Change Req
(2) Interim Update (Optional UDRs)

Figure 4-33 – 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.

4.4.3.4.7.4 Network Exit

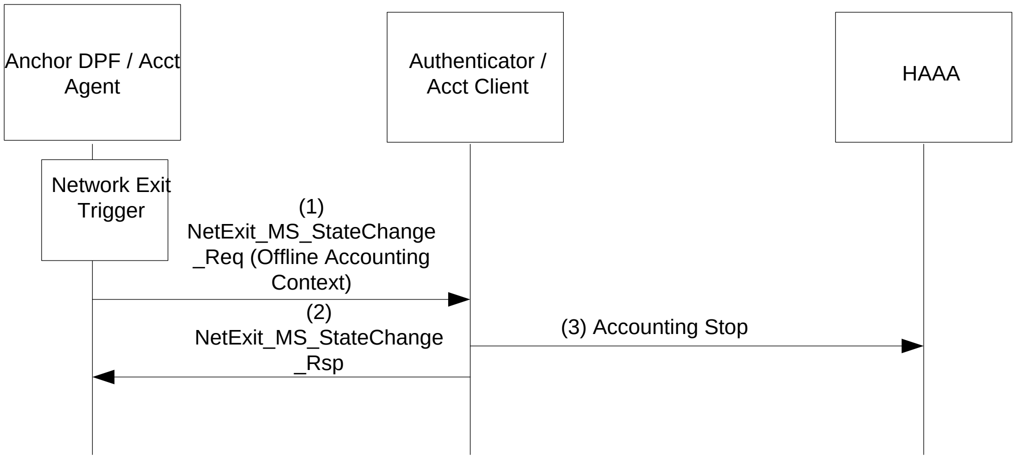

Anchor DPF / Acct Agent
Authenticator / Acct Client
HAAA
Network Exit Trigger
(1) NetExit_MS_StateChange _Req (Offline Accounting Context)
(2) NetExit_MS_StateChange _Rsp
(3) Accounting Stop

Figure 4-34 – 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.

4.4.3.4.8 Accounting Client Relocation

Accounting Client is collocated with MS/AMS 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.

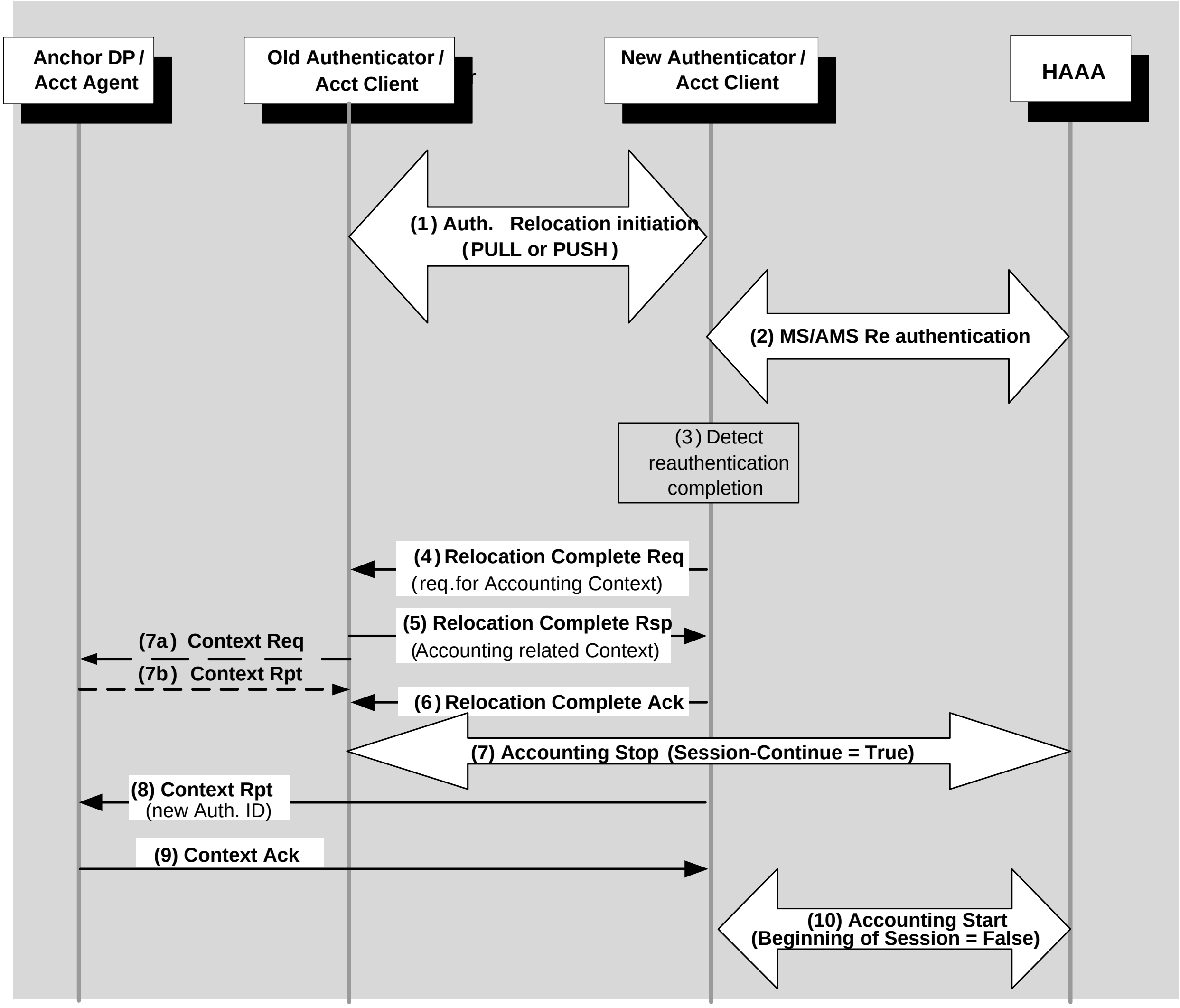

Anchor DP / Acct Agent
Old Authenticator / Acct Client
New Authenticator / Acct Client
HAAA
(1) Auth. Relocation initiation (PULL or PUSH)
(2) MS/AMS Re authentication
(3) Detect reauthentication completion
(4) Relocation Complete Req (req.for Accounting Context)
(5) Relocation Complete Rsp (Accounting related Context)
(7a) Context Req
(7b) Context Rpt
(6) Relocation Complete Ack
(7) Accounting Stop (Session-Continue = True)
(8) Context Rpt (new Auth. ID)
(9) Context Ack
(10) Accounting Start (Beginning of Session = False)

Figure 4-35 – Accounting Client relocation

STEP 1

Authenticator relocation is initiated (PUSH or PULL modes).

STEP 2

MS/AMS Reauthentication occurs in the “new” Authenticator entity. This includes EAP Phase and PKMv2/PKMv3 3WHS Phase.

STEP 3

In the case the “new” Authenticator detects successful completion of reauthentication process (successful completion of PKMv2/PKMv3 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_R*sp 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.

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).

Table 4-33 – 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	

IE	Reference	M/O	Notes
>>>>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	

4.4.3.4.9 Accounting Agent Relocation

Accounting Agent is collocated with MS/AMS 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 [4.8.2.3.8]. 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.

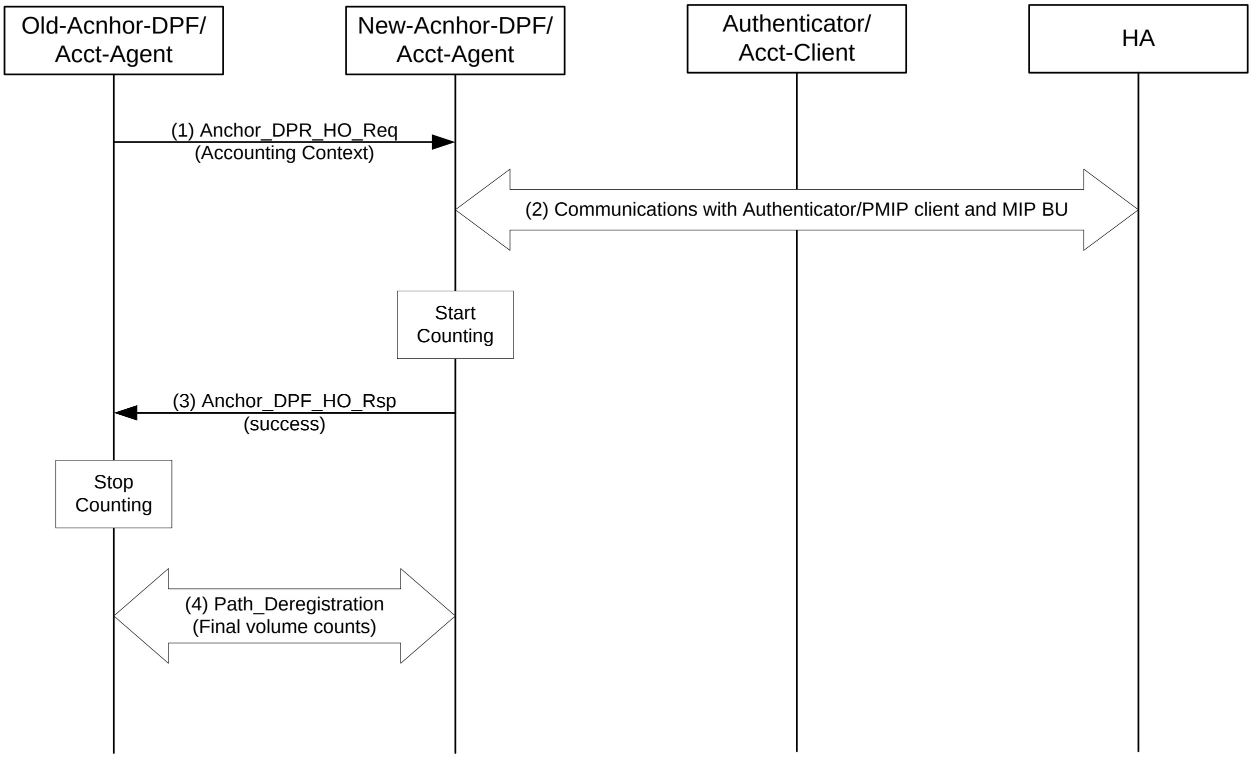

Old-Acnhor-DPF/ Acct-Agent
New-Acnhor-DPF/ Acct-Agent
Authenticator/ Acct-Client
HA
(1) Anchor_DPR_HO_Req (Accounting Context)
(2) Communications with Authenticator/PMIP client and MIP BU
Start Counting
(3) Anchor_DPF_HO_Rsp (success)
Stop Counting
(4) Path_Deregistration (Final volume counts)

Figure 4-36 – 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 [4.8.2.3.8].

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 Hot-lining

As indicated in WiMAX Forum® Network Architecture 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 WiMAX Forum® Network Architecture 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 4-37 depicts the call flow between the HLD, HAAA and HLA.

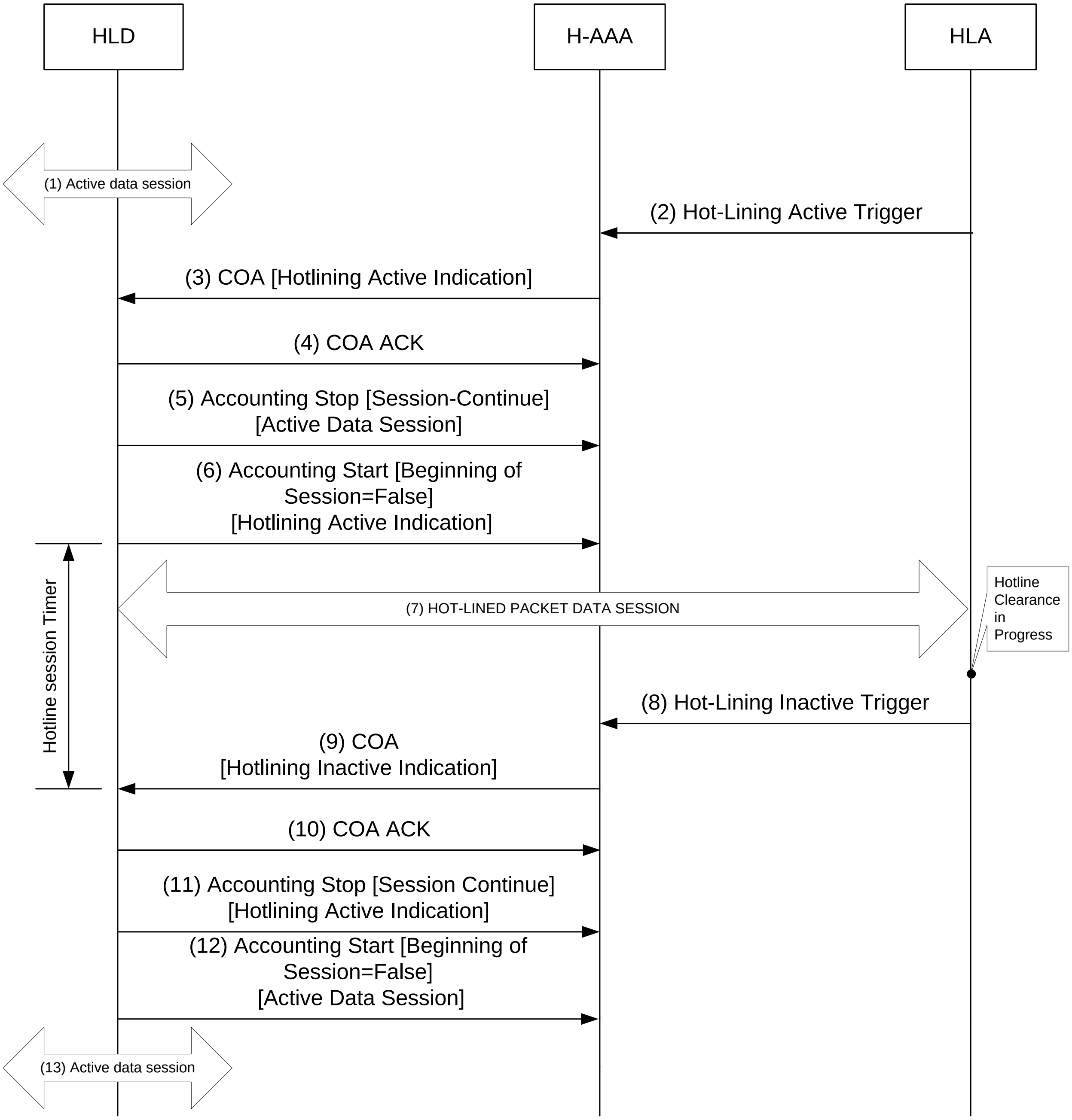

HLD
H-AAA
HLA
(1) Active data session
(2) Hot-Lining Active Trigger
(3) COA [Hotlining Active Indication]
(4) COA ACK
(5) Accounting Stop [Session-Continue] [Active Data Session]
(6) Accounting Start [Beginning of Session=False] [Hotlining Active Indication]
Hotline session Timer
(7) HOT-LINED PACKET DATA SESSION
Hotline Clearance in Progress
(8) Hot-Lining Inactive Trigger
(9) COA [Hotlining Inactive Indication]
(10) COA ACK
(11) Accounting Stop [Session Continue] [Hotlining Active Indication]
(12) Accounting Start [Beginning of Session=False] [Active Data Session]
(13) Active data session

Figure 4-37 – 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 0.

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.

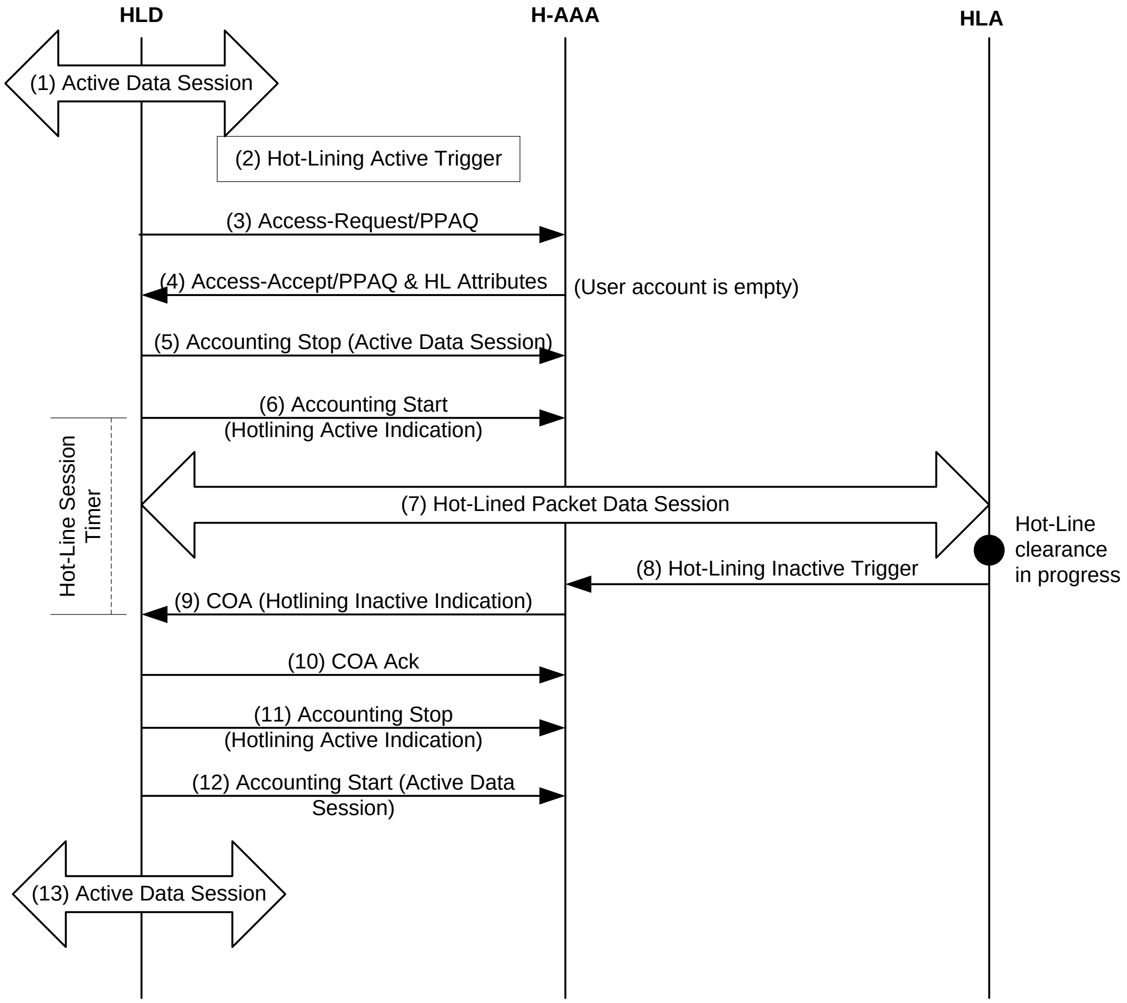

HLD
H-AAA
HLA
(1) Active Data Session
(2) Hot-Lining Active Trigger
(3) Access-Request/PPAQ
(4) Access-Accept/PPAQ & HL Attributes
(User account is empty)
(5) Accounting Stop (Active Data Session)
(6) Accounting Start
(Hotlining Active Indication)
Hot-Line Session Timer
(7) Hot-Lined Packet Data Session
Hot-Line clearance in progress
(8) Hot-Lining Inactive Trigger
(9) COA (Hotlining Inactive Indication)
(10) COA Ack
(11) Accounting Stop
(Hotlining Active Indication)
(12) Accounting Start (Active Data Session)
(13) Active Data Session

Figure 4-38 – 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 4-37.

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 4-39 depicts the call flow between the HLD, HAAA and HLA.

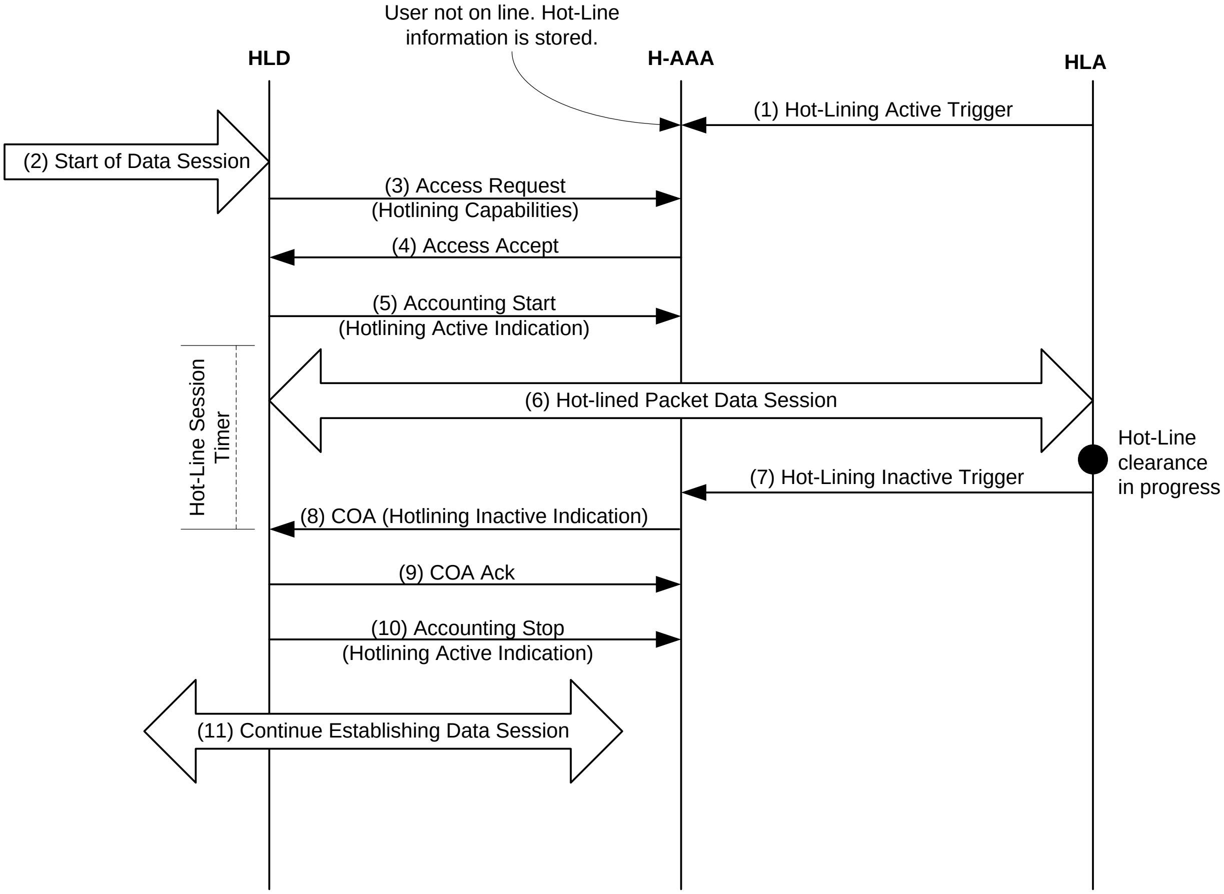

User not on line. Hot-Line information is stored.
HLD
H-AAA
HLA
(1) Hot-Lining Active Trigger
(2) Start of Data Session
(3) Access Request (Hotlining Capabilities)
(4) Access Accept
(5) Accounting Start (Hotlining Active Indication)
Hot-Line Session Timer
(6) Hot-lined Packet Data Session
Hot-Line clearance in progress
(7) Hot-Lining Inactive Trigger
(8) COA (Hotlining Inactive Indication)
(9) COA Ack
(10) Accounting Stop (Hotlining Active Indication)
(11) Continue Establishing Data Session

Figure 4-39 – 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 it Hot-Line capability in the 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 with Beginning-of-Session set to True. 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 with session-continue set to True.

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/ABS that does not belong to the network entry zone of the MS/AMS.

Figure 4-40 depicts the call flows between the HLD, HAAA and HLA.

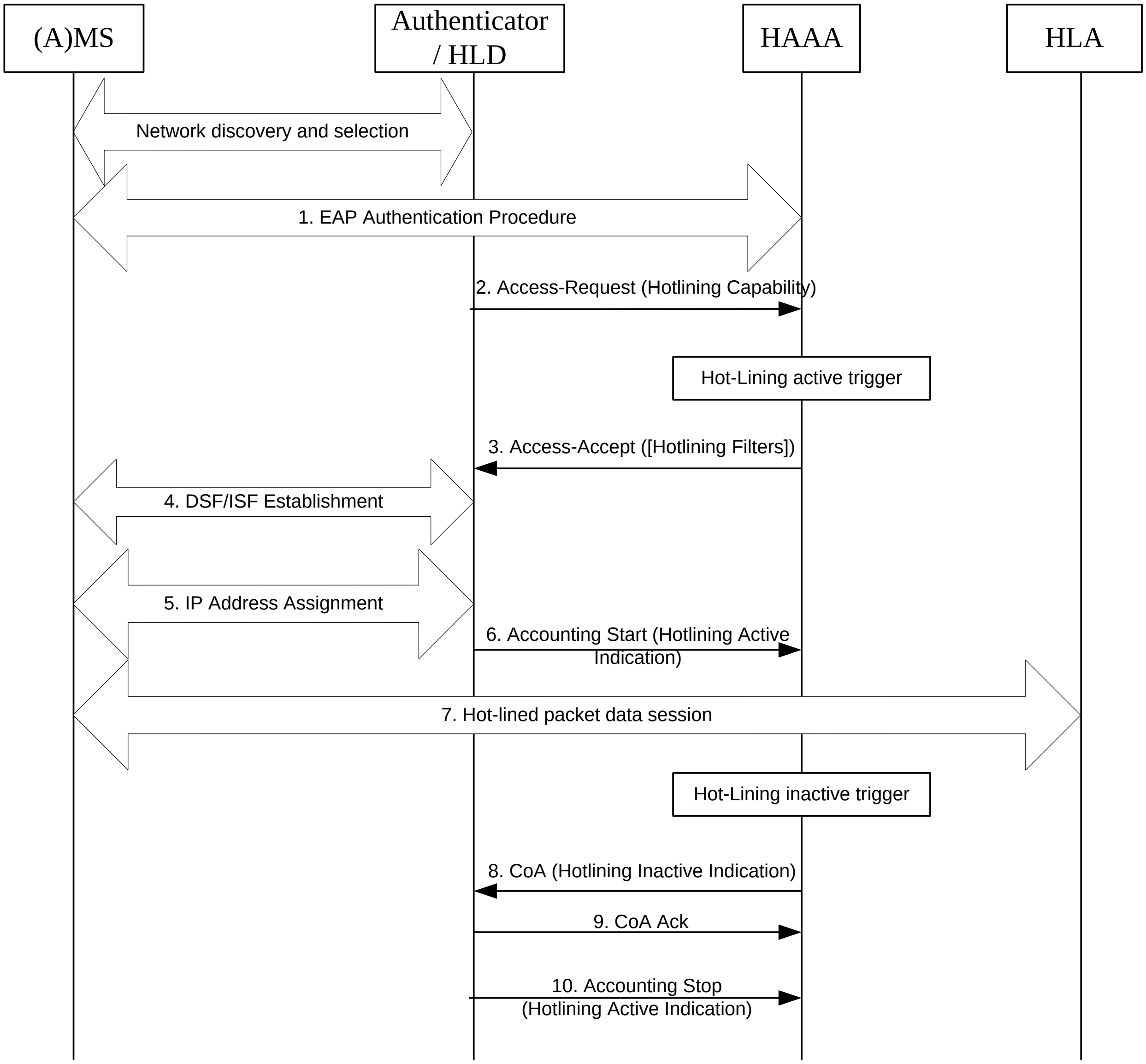

(A)MS
Authenticator / HLD
HAAA
HLA
Network discovery and selection
1. EAP Authentication Procedure
2. Access-Request (Hotlining Capability)
Hot-Lining active trigger
3. Access-Accept ([Hotlining Filters])
4. DSF/ISF Establishment
5. IP Address Assignment
6. Accounting Start (Hotlining Active Indication)
7. Hot-lined packet data session
Hot-Lining inactive trigger
8. CoA (Hotlining Inactive Indication)
9. CoA Ack
10. Accounting Stop (Hotlining Active Indication)

Figure 4-40 – Hot-lining during initial network entry

STEP 1

The MS/AMS 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) or default service flow(DSF) for the MS/AMS.

STEP 5

The MS/AMS 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) with Beginning-of-Session set to True 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 with session-continue set to True to indicate the inactivation of the Hot-lining.

4.4.3.5.4 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.

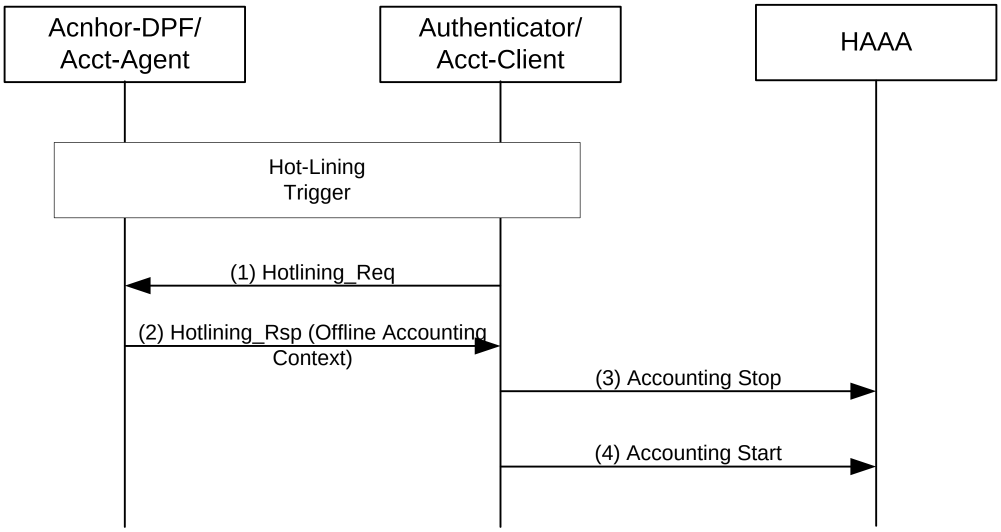


Figure 4-41 – Context Update procedure

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 / DCR_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 , *IM_Exit_State_Change_Rsp* during Idle Mode Exit and DCR_Exit_State_Change_Rsp during DCR Mode Exit. The TLV is included only once even if multiple flows are included in the message.

Table 4-34 – RR_Req (Create) / HO_Req / Anchor_DPF_HO_Req (for R4 only) / Context_Rpt / IM_Exit_State_Change_Rsp/ DCR_Exit_State_Change_Rsp Message Structure

IE	Description	M/O	Notes
…			For a complete list of the additional IEs in the RR_Req message, see Table 4-60 and Table 4-61 for R4. For a complete list of the additional IEs in the HO_Req message, see Table 4-83. For a complete list of the additional IEs in the Anchor_DPF_HO_Req message, see Table 4-115 and Table 4-135. Anchor_DPF_HO_Req applies to R4 only. For a complete list of the additional IEs in the Context_Rpt message, see Table 4-20, Table 4-85, Table 4-94, Table 4-158 and Table 4-180 for R4. For a complete list of the additional IEs in the IM_Exit_State_Change_Rsp message, see Table 4-176 for R4 and Table 4-173 for R6. For a complete list of the additional IEs in the DCR_Exit_State_Change_Rsp message, see Table 4-xxx for R4 and Table 4-xxx for R6.
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, exiting idle mode and exiting DCR 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 Access_Accept message. This TLV is only used for volume-based accounting. This TLV SHALL be included in Anchor_DPF_HO_Req messages. Anchor_DPF_HO_Req 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 Access-Accept packet. 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 message.

IE	Description	M/O	Notes
>>>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 4-35 – RR_Rsp (Modify and Delete) Message Structure

IE	Description	M/O	Notes
…			For a complete list of the additional IEs in the RR_Rsp 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.
>>>>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	

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/ABS to the serving ASN-GW. The Ack message does not contain any TLVs, it is just a confirmation to the BS/ABS 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/AMS based on the corresponding MSID and the accounting granularity.

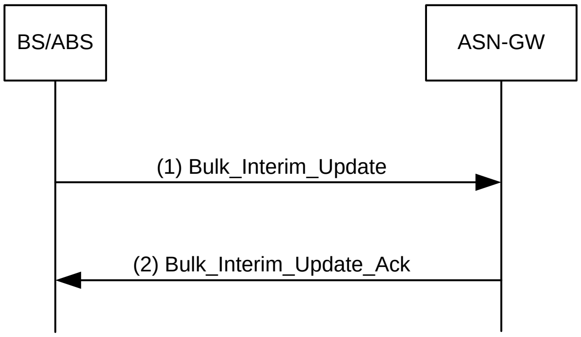


Figure 4-42 – Bulk Interim Update

Table 4-36 – 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	
>>Accounting Number of Bulk Sessions	5.3.2.245	M	

IE	Description	M/O	Notes
>>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 / DCR_Entry_State_Change_Req / NetExit_MS_State_Change_Req/Rsp

R6 *Path_Dereg_Req* and R6 *IM_Entry_State_Change_Req* and R6 *DCR_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 and DCR Mode Entry MS/AMS de-registration from the network and MS/AMS Network Exit procedures. The *Path_Dereg_Req/IM_Entry_State_Change_Req/ DCR_Entry_State_Change_Req / NetExit_MS_State_Change_Req/Rsp* message structure is described in Table 4-37.

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/ DCR_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*, *IM_Exit_State_Change_Rsp* during Idle Mode Exit and *DCR_Exit_State_Change_Rsp* during DCR 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* / *DCR_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/ABS 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 / DCR_Entry_State_Change_Req / NetExit_MS_State_Change_Req/Rsp

R4 *Path_Dereg_Req* and R4 *IM_Entry_State_Change_Req* and R4 *DCR_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 and DCR Mode Entry MS/AMS de-registration from the network and MS/AMS Network Exit procedures.

Table 4-37 – Path_Dereg_Req / IM_Entry_State_Change_Req / *DCR_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 DCR_Entry_State_Change_Req message, see Table 4-xxx for R4 and Table 4-xxx 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.

IE	Description	M/O	Notes
>>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	
>>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 and DCR Mode Entry MS/AMS de-registration from the network and MS/AMS 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.

IE	Description	M/O	Notes
>>>>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	

4.4.3.6.2.5 Prepaid_Request / Prepaid_Notify Messages

These messages are used over R4 for online accounting events communication between PPA and PPC (quota requests and quota updates). *Prepaid Request* message SHALL include PPAQ (quota) TLV. *Prepaid Notify* message SHALL include PPAQ (quota) TLV if quota update is performed. In the case there is no additional resources for the particular service, PPC sends *Prepaid Notify* message to PPA without PPAQ.

Table 4-38 – 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	

IE	Reference	M/O	Notes
>>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.

Table 4-39 – 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:

- $T_{Prepaid\_Request}$: 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 4-40 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-40 – Timer Values for Prepaid Messages over R4

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{Prepaid\_Request}$	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 4-41 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 4-41 Timer Expiry Conditions.

Table 4-41 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{Prepaid\_Request}$	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 4-42 – 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.

IE	Description	M/O	Notes
> Service-Id	5.3.2.280	O	Used to identify the Hotlining Context on the Expiry of PPAQ with Same Service ID.

1

2 **Table 4-43 – 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	

IE	Description	M/O	Notes
>>>>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	

4.4.3.7 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/AMS.

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/AMS. 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/AMS.

b. Upon successful modification of an ongoing mobility binding for an MS/AMS (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/AMS.

b. Upon successful modification of an ongoing mobility binding for an MS/AMS (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.

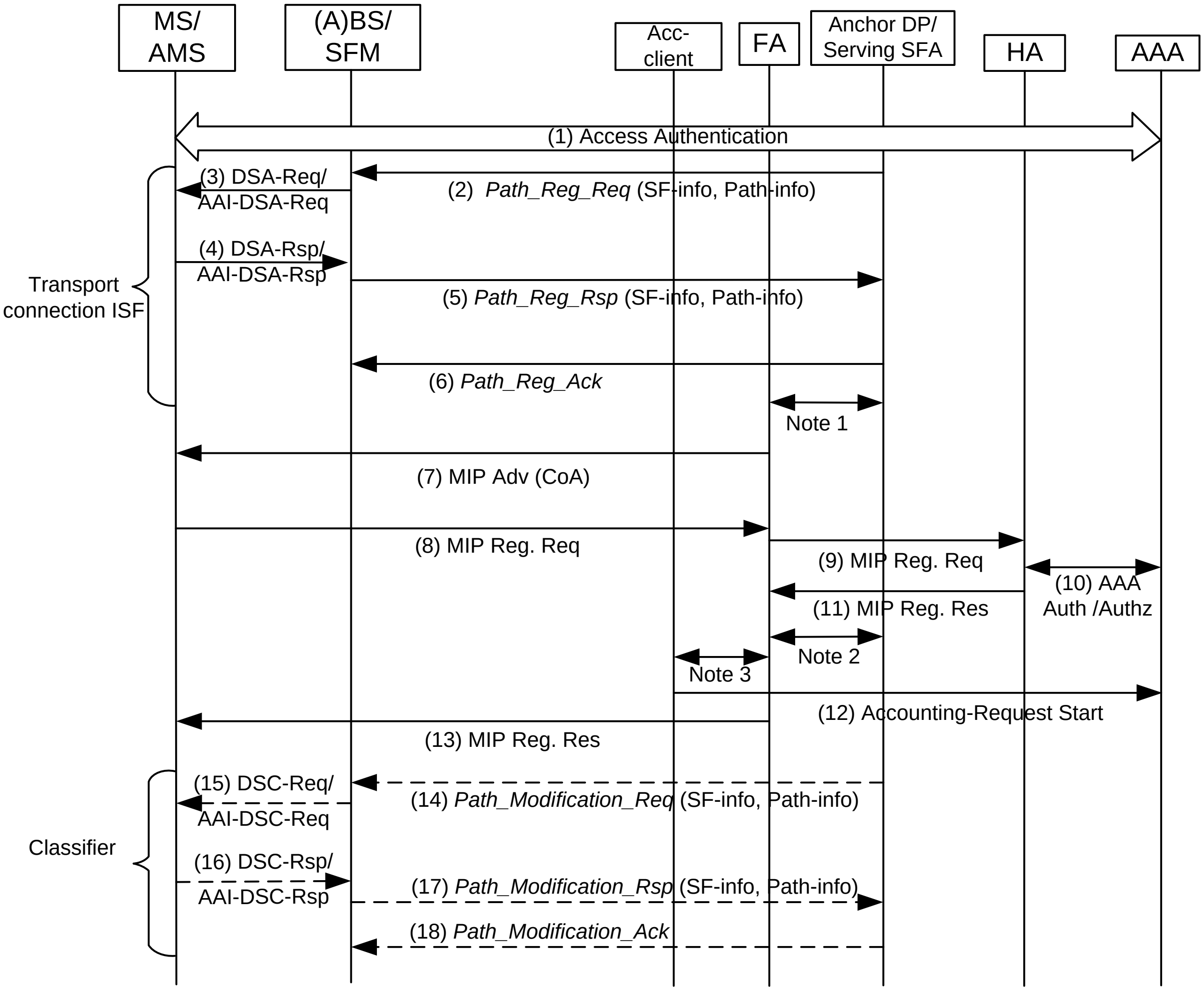
e. At the reset of Hot-Lining of an ongoing IP session.

f. Due to overflow of any of the counters.

4.4.3.9 Illustrations of the Accounting Start Events in the ASN

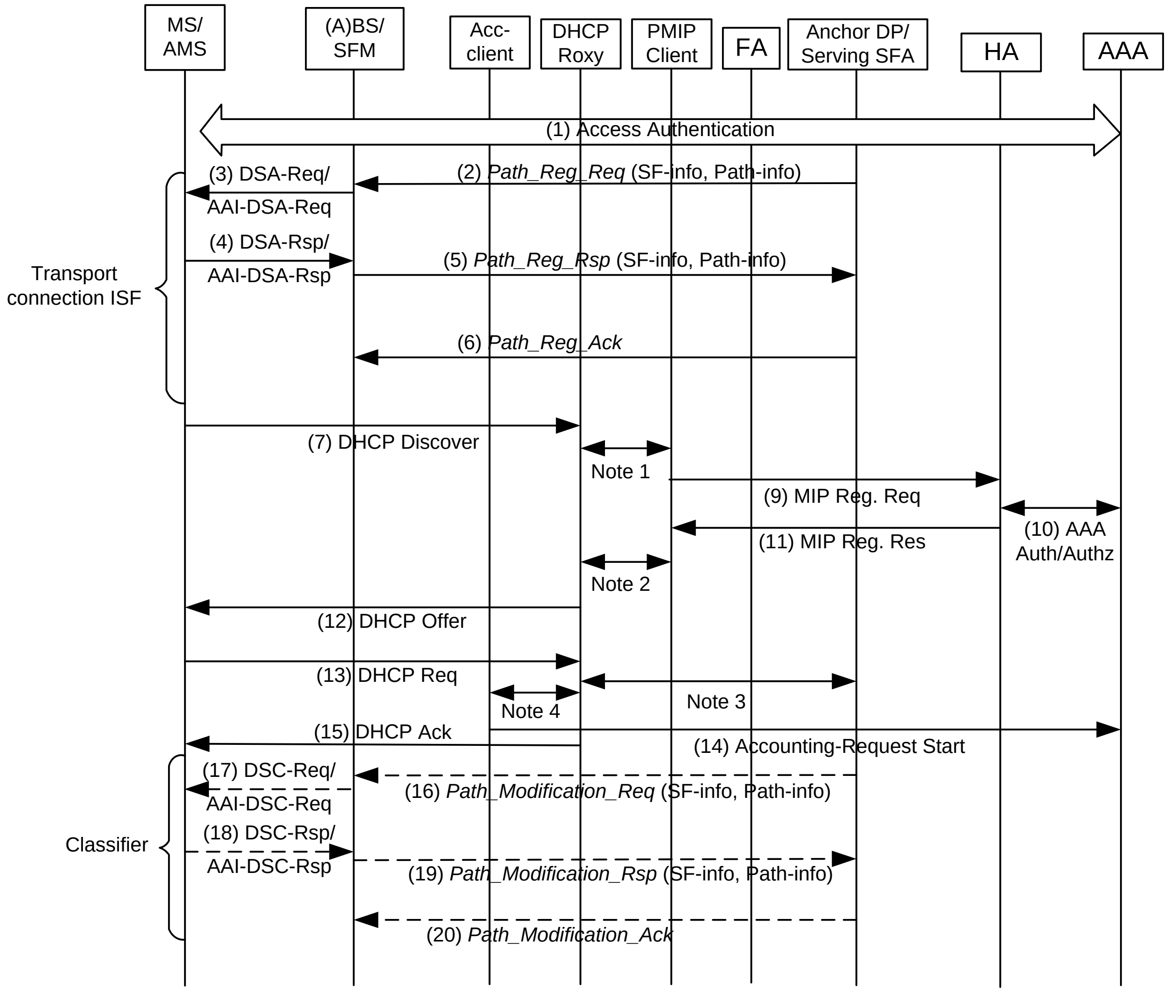
The purpose of the figures in this section is to contextualize the accounting triggers. The figures are informative. For further details refer to the specific sections in this document.

For the case that FIAA is not applied Figure 4-43 to Figure 4-48 are available also. The case that FIAA is applied is depicted in Figure 4-49.



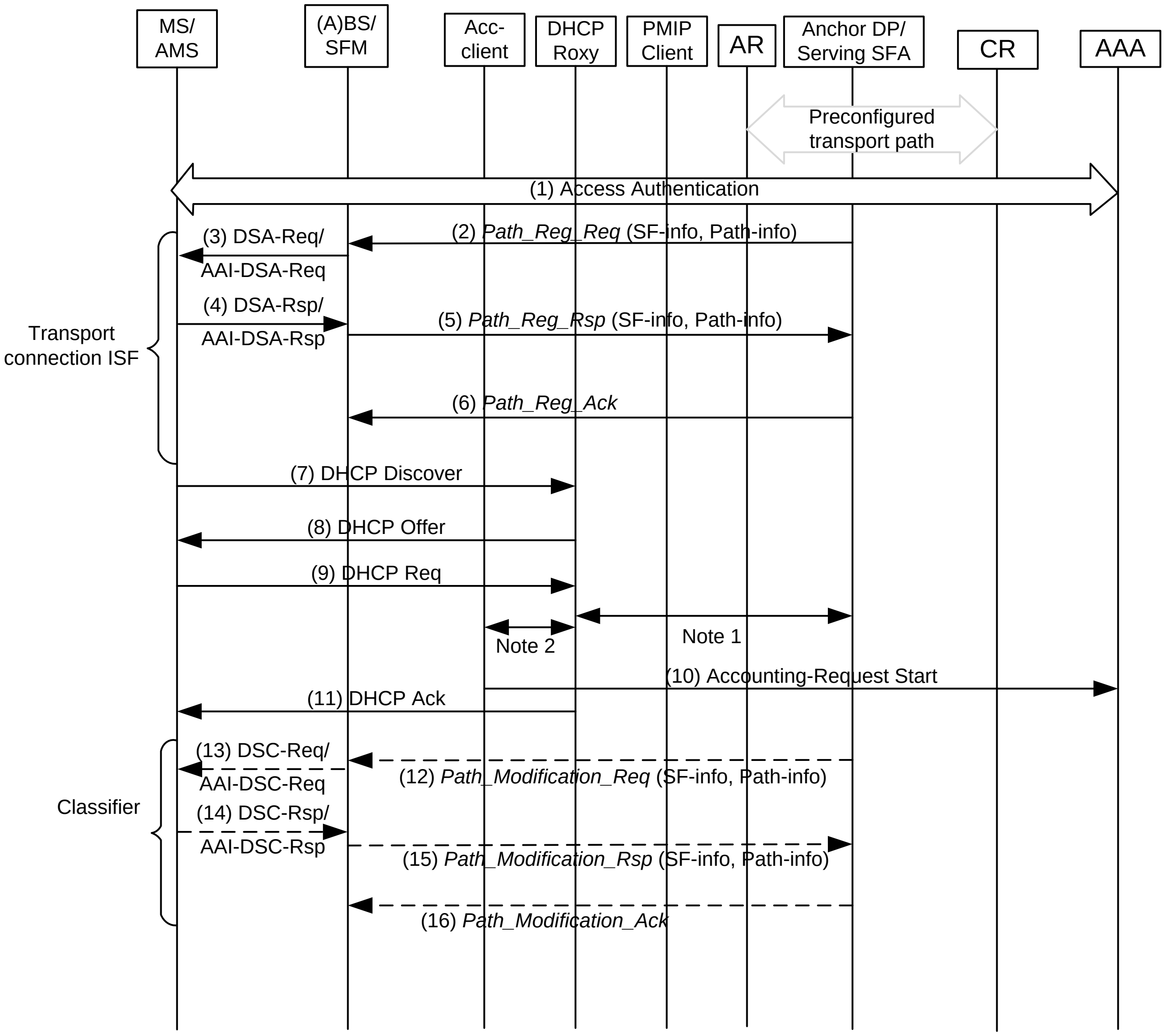
Note 1: Serving SFA triggers FA to initiate MIP registration (out of scope of spec)
Note 2: FA triggers the Anchor DP/Serving SFA to update the SF classifier. (out of scope of spec)
Note 3: FA triggers the Acc client to generate Accounting-Request Start (out of scope of spec)

Figure 4-43 – Accounting Start Event in the ASN in Case of CMIP4



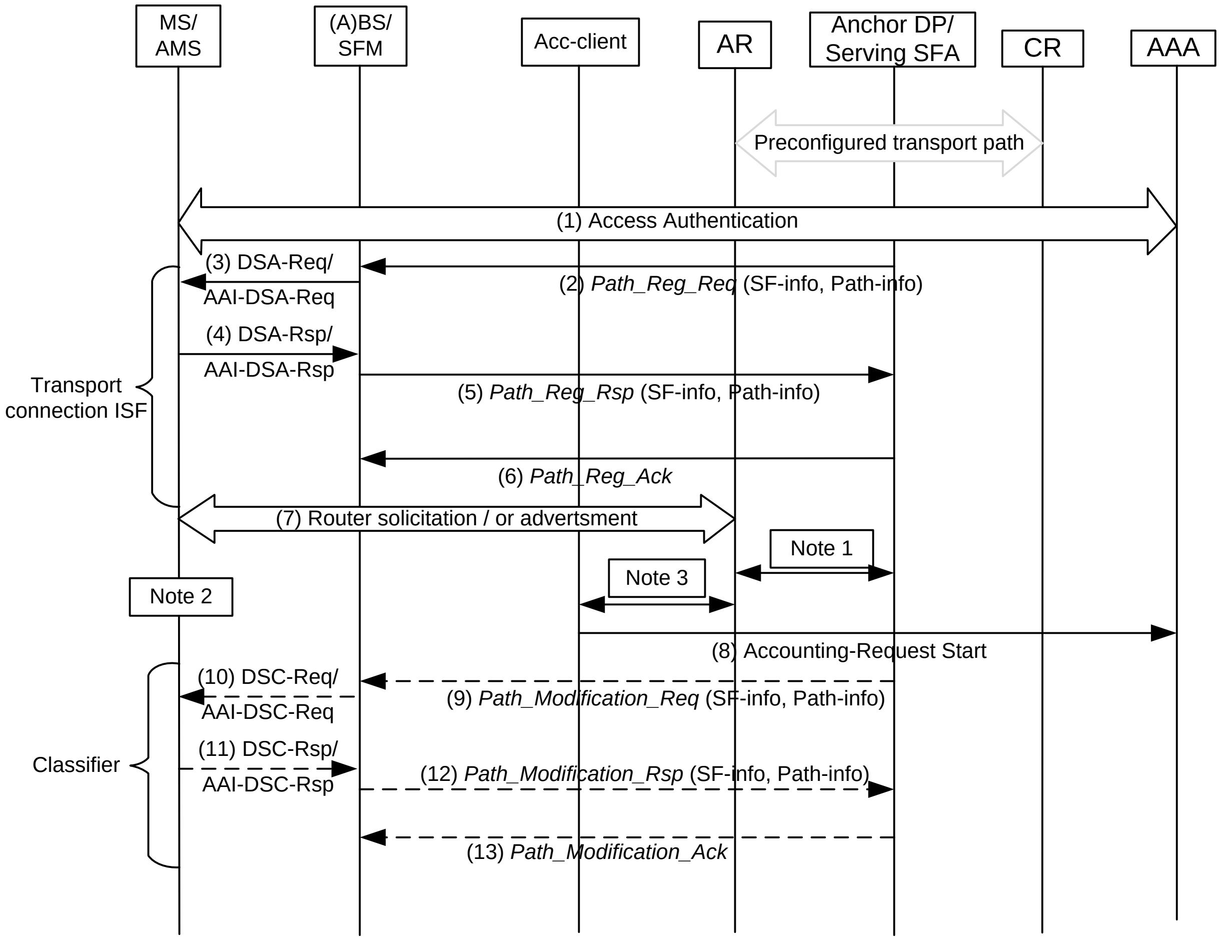
Note 1: DHCP Proxy trigger PMIP client to initiate MIP registration (out of scope of this section)
Note 2: PMIP client trigger the DHCP proxy and passes MIP registration response information. (out of scope of this section)
Note 3: DHCP proxy triggers the Anchor DP/Serving SFA to update the SF classifier. (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 4-44 – Accounting Start Event in the ASN in Case of PMIP4


MS/ AMS
(A)BS/ SFM
Acc-client
DHCP Roxy
PMIP Client
AR
Anchor DP/ Serving SFA
CR
AAA
Preconfigured transport path
(1) Access Authentication
(2) Path_Reg_Req (SF-info, Path-info)
(3) DSA-Req/ AAI-DSA-Req
(4) DSA-Rsp/ AAI-DSA-Rsp
(5) Path_Reg_Rsp (SF-info, Path-info)
Transport connection ISF
(6) Path_Reg_Ack
(7) DHCP Discover
(8) DHCP Offer
(9) DHCP Req
Note 2
Note 1
(10) Accounting-Request Start
(11) DHCP Ack
(13) DSC-Req/ AAI-DSC-Req
(12) Path_Modification_Req (SF-info, Path-info)
Classifier
(14) DSC-Rsp/ AAI-DSC-Rsp
(15) Path_Modification_Rsp (SF-info, Path-info)
(16) Path_Modification_Ack

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 4-45 – Accounting Start Event in the ASN in Case of Simple IPv4

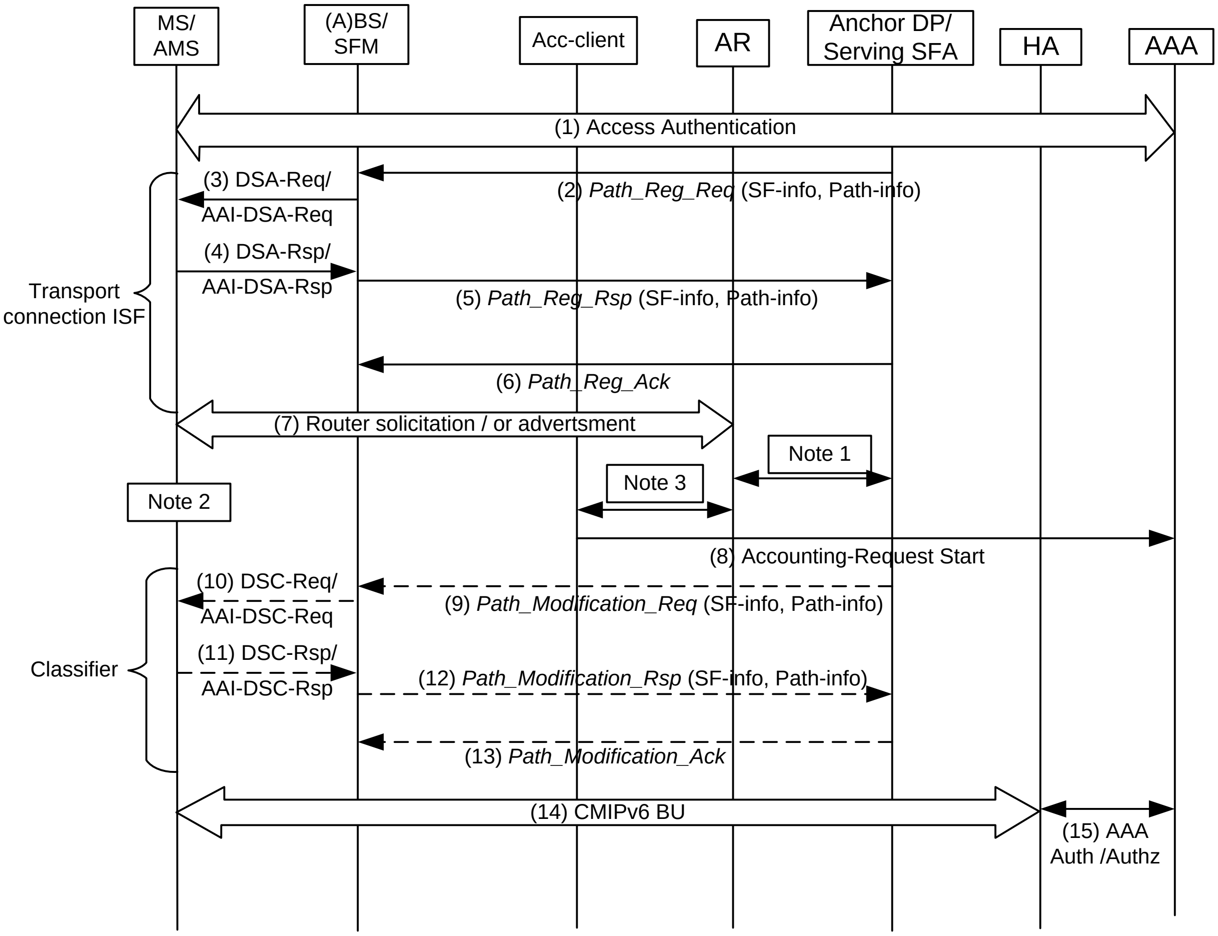

MS/
AMS
(A)BS/
SFM
Acc-client
AR
Anchor DP/
Serving SFA
CR
AAA
Preconfigured transport path
(1) Access Authentication
(2) Path_Reg_Req (SF-info, Path-info)
(3) DSA-Req/
AAI-DSA-Req
(4) DSA-Rsp/
AAI-DSA-Rsp
(5) Path_Reg_Rsp (SF-info, Path-info)
Transport
connection ISF
(6) Path_Reg_Ack
(7) Router solicitation / or advertsment
Note 1
Note 3
Note 2
(8) Accounting-Request Start
(9) Path_Modification_Req (SF-info, Path-info)
(10) DSC-Req/
AAI-DSC-Req
(11) DSC-Rsp/
AAI-DSC-Rsp
Classifier
(12) Path_Modification_Rsp (SF-info, Path-info)
(13) Path_Modification_Ack

Note 1: AR in the ASN triggers the Anchor DP / Serving SFA to update the SF classifier, with IPv6 Prefix (64 bits) (out of scope)

Note 2: Address Auto-configure and DAD occurs after the router solicitation, advertisement, and DAD.

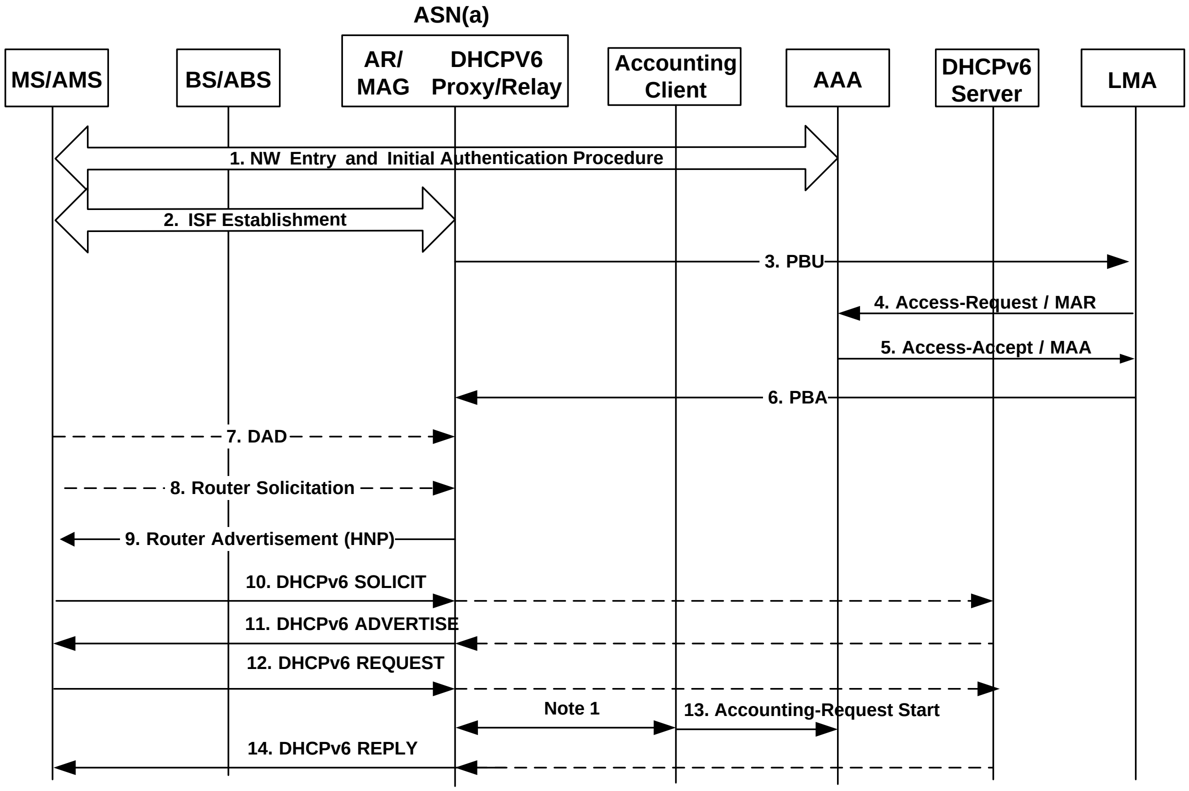
Note 3: AR triggers the Acc Client to generate Accounting-Request Start (out of scope)

Figure 4-46 – Accounting Start Event in the ASN in Case of Simple IPv6


MS/ AMS
(A)BS/ SFM
Acc-client
AR
Anchor DP/ Serving SFA
HA
AAA
(1) Access Authentication
(2) *Path_Reg_Req* (SF-info, Path-info)
(3) DSA-Req/ AAI-DSA-Req
(4) DSA-Rsp/ AAI-DSA-Rsp
(5) *Path_Reg_Rsp* (SF-info, Path-info)
Transport connection ISF
(6) *Path_Reg_Ack*
(7) Router solicitation / or advertsment
Note 1
Note 3
Note 2
(8) Accounting-Request Start
(10) DSC-Req/ AAI-DSC-Req
(9) *Path_Modification_Req* (SF-info, Path-info)
(11) DSC-Rsp/ AAI-DSC-Rsp
Classifier
(12) *Path_Modification_Rsp* (SF-info, Path-info)
(13) *Path_Modification_Ack*
(14) CMIPv6 BU
(15) AAA Auth /Authz

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 4-47 – 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 4-48 – Accounting Start Event in the ASN in case of PMIP6

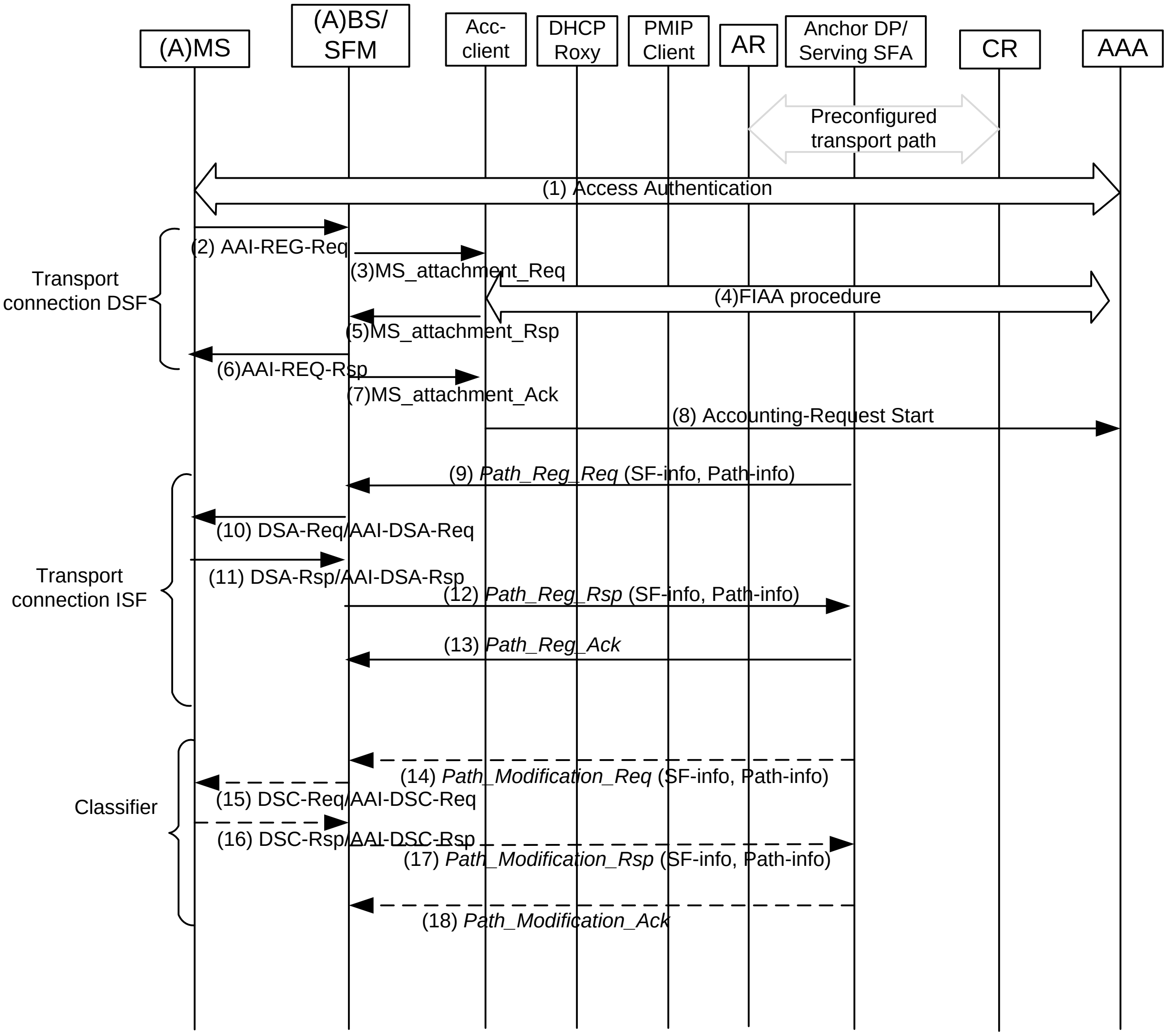


Figure 4-49 – Accounting Start Event in the ASN in case that FIAA is applied

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.

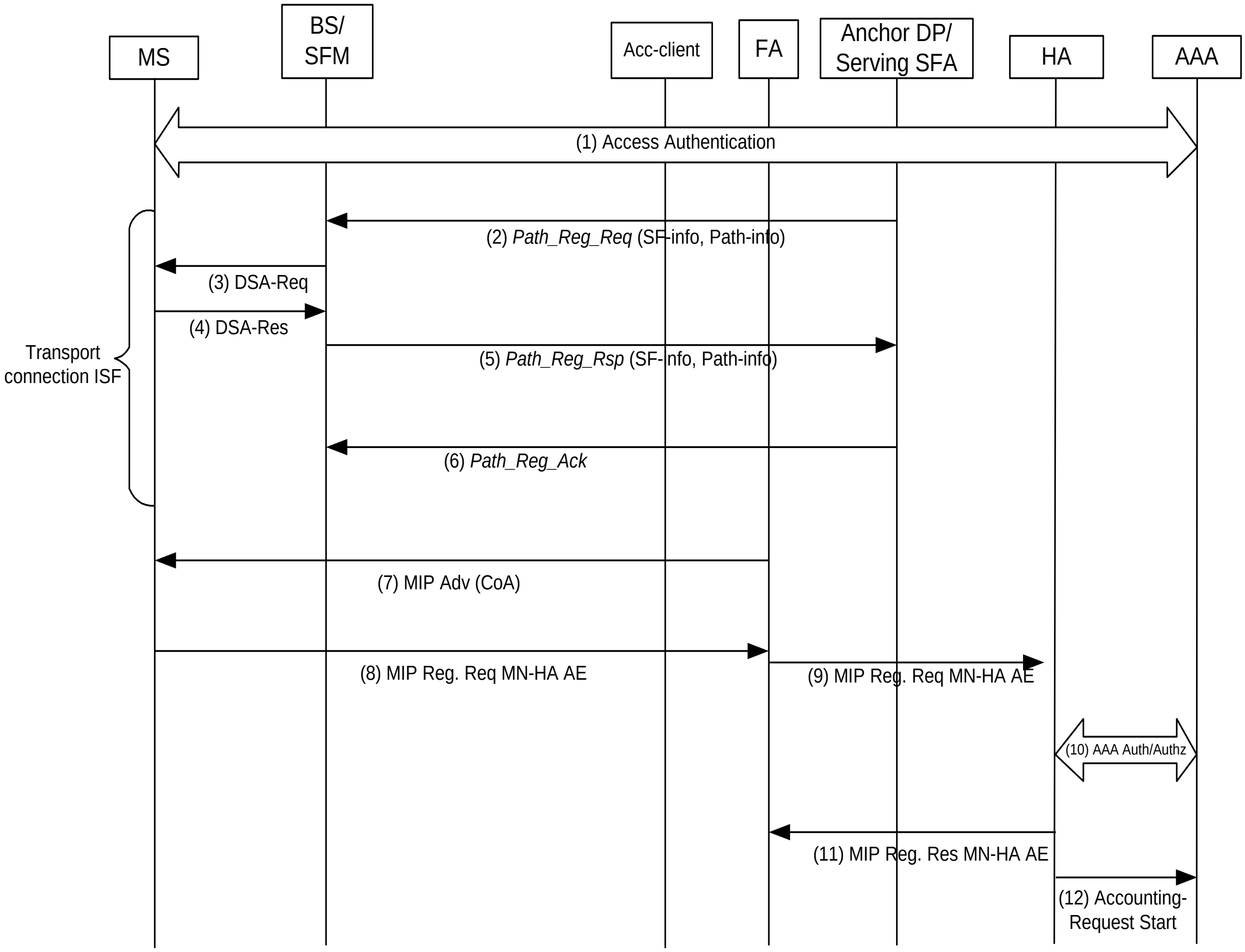

MS
BS/ SFM
Acc-client
FA
Anchor DP/ Serving SFA
HA
AAA
(1) Access Authentication
Transport connection ISF
(2) *Path_Reg_Req* (SF-info, Path-info)
(3) DSA-Req
(4) DSA-Res
(5) *Path_Reg_Rsp* (SF-info, Path-info)
(6) *Path_Reg_Ack*
(7) MIP Adv (CoA)
(8) MIP Reg. Req MN-HA AE
(9) MIP Reg. Req MN-HA AE
(10) AAA Auth/Authz
(11) MIP Reg. Res MN-HA AE
(12) Accounting-Request Start

Figure 4-50 – Accounting Start Event in the CSN in Case of CMIP4

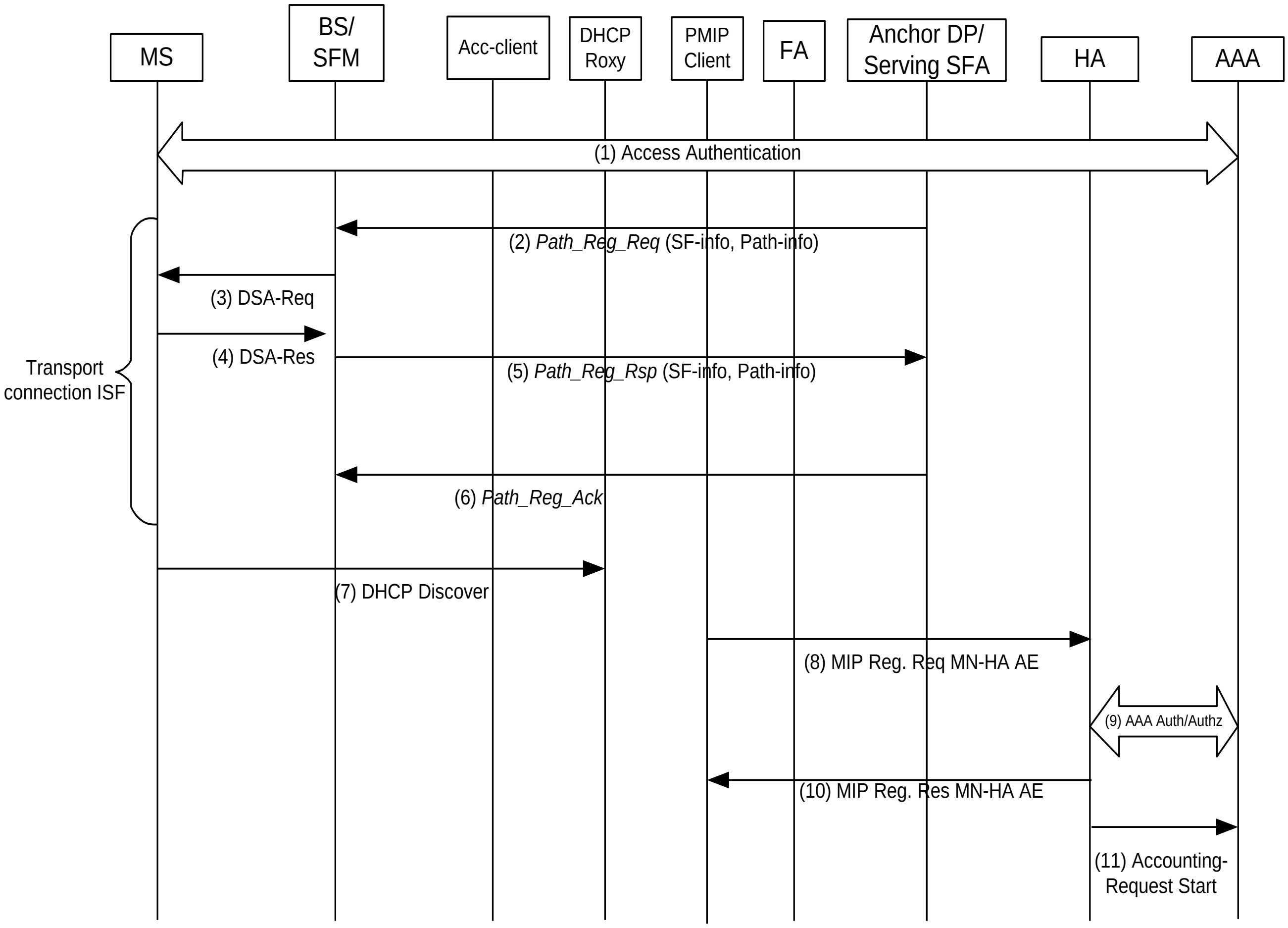

MS
BS/ SFM
Acc-client
DHCP Roxy
PMIP Client
FA
Anchor DP/ Serving SFA
HA
AAA
(1) Access Authentication
(2) Path_Reg_Req (SF-info, Path-info)
(3) DSA-Req
(4) DSA-Res
(5) Path_Reg_Rsp (SF-info, Path-info)
Transport connection ISF
(6) Path_Reg_Ack
(7) DHCP Discover
(8) MIP Reg. Req MN-HA AE
(9) AAA Auth/Authz
(10) MIP Reg. Res MN-HA AE
(11) Accounting-Request Start

Figure 4-51 – Accounting Start Event in the CSN in Case of PMIP4

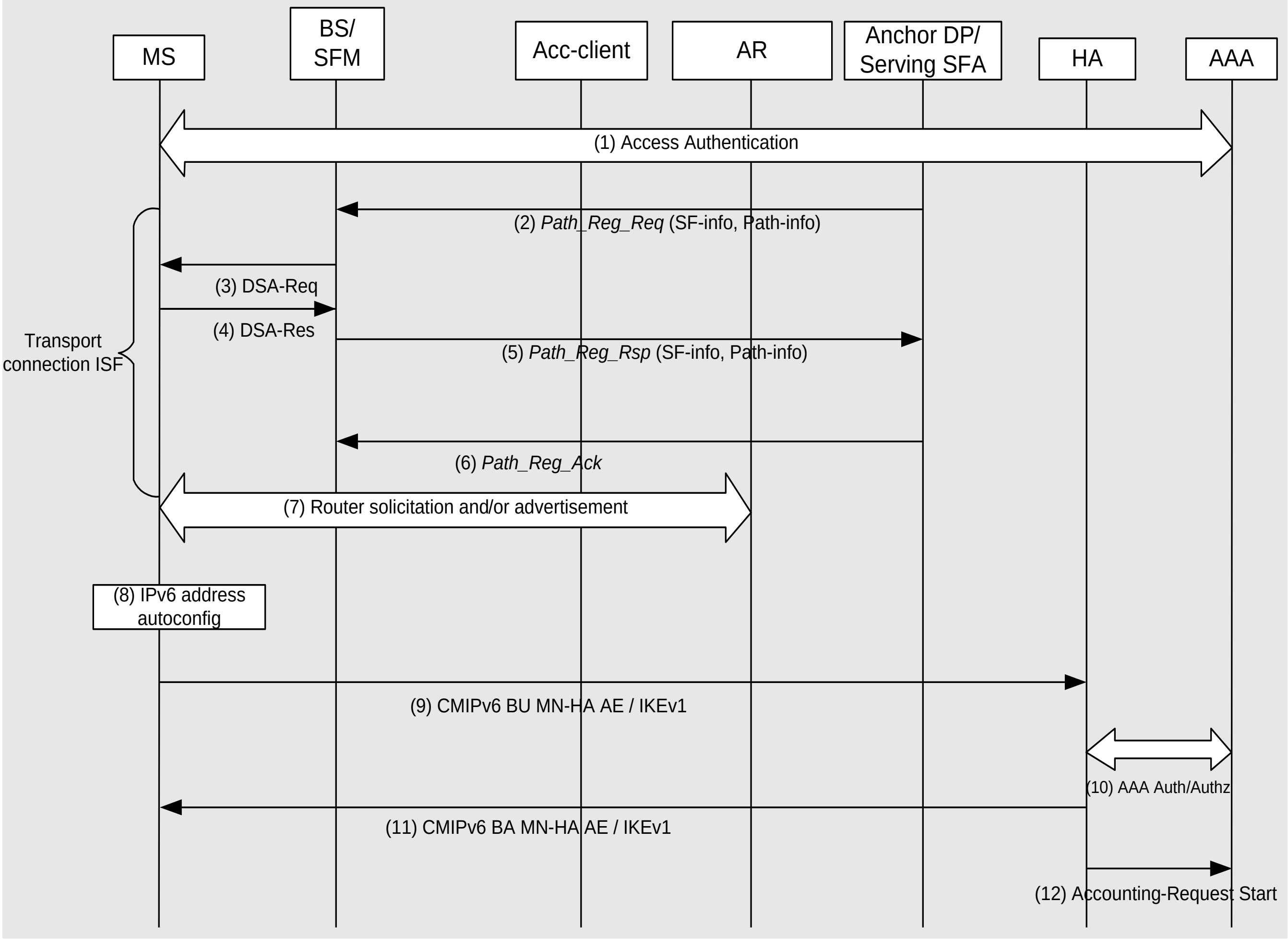

BS/ SFM
MS
Acc-client
AR
Anchor DP/ Serving SFA
HA
AAA
(1) Access Authentication
(2) Path_Reg_Req (SF-info, Path-info)
(3) DSA-Req
(4) DSA-Res
Transport connection ISF
(5) Path_Reg_Rsp (SF-info, Path-info)
(6) Path_Reg_Ack
(7) Router solicitation and/or advertisement
(8) IPv6 address autoconfig
(9) CMIPv6 BU MN-HA AE / IKEv1
(10) AAA Auth/Authz
(11) CMIPv6 BA MN-HA AE / IKEv1
(12) Accounting-Request Start

Figure 4-52 – Accounting Start Event in the CSN in Case of CMIP6

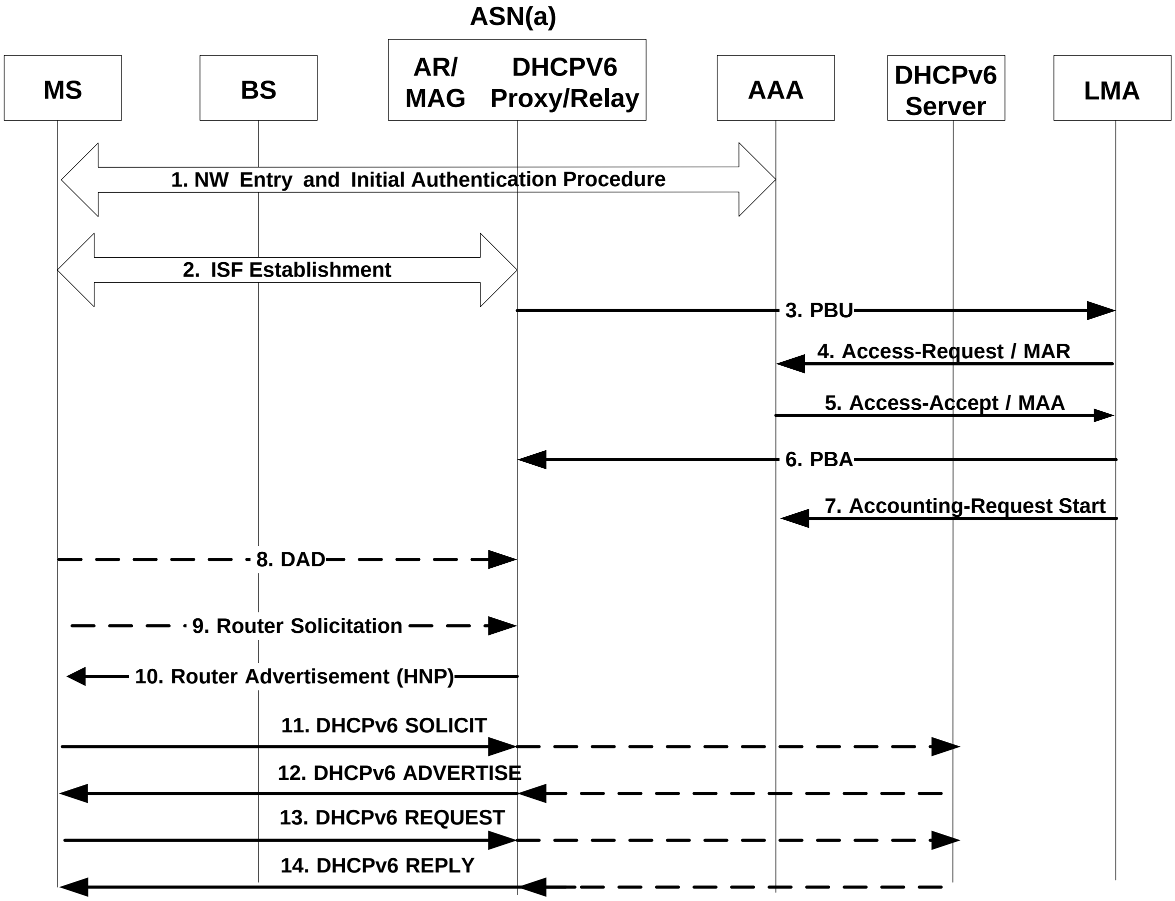


Figure 4-53 – Accounting Start Event in the CSN in Case of PMIP6

4.5 Network Entry and Exit

4.5.1 MS/AMS-to-Network Initial Authentication Flow

4.5.1.1 Single EAP

4.5.1.1.1 Network entry in BS/ABS(LZone)

Figure 4-55 – AMS Initial Network Entry in ABS(MZone) (Single EAP)

describes normative procedures for an initial MS/AMS network entry focusing on MS-to-Network EAP authentication process (single EAP) and MS 802.16e registration.

The BS/ABS 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.

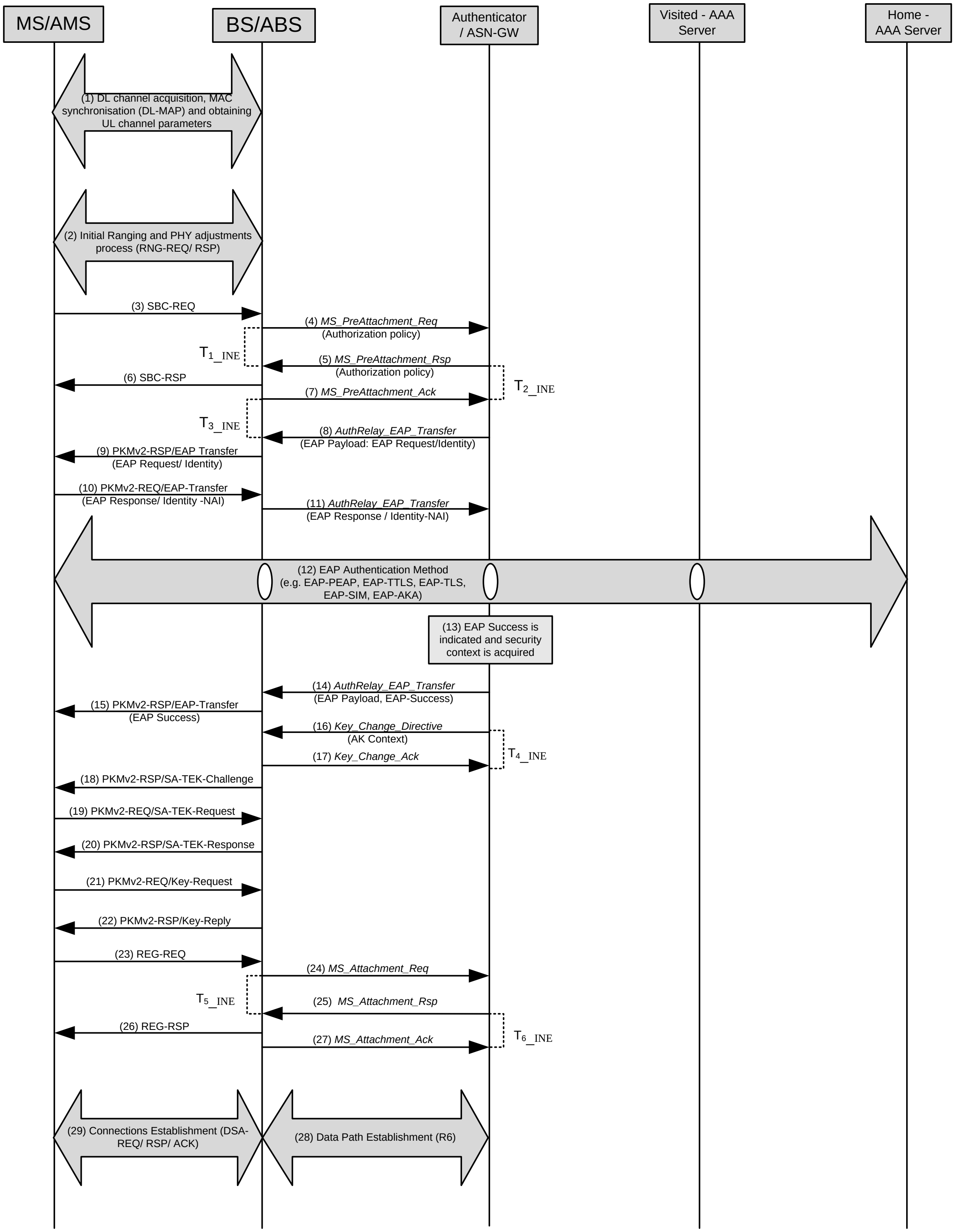

MS/AMS
BS/ABS
Authenticator / ASN-GW
Visited - AAA Server
Home - AAA Server
(1) DL channel acquisition, MAC synchronisation (DL-MAP) and obtaining UL channel parameters
(2) Initial Ranging and PHY adjustments process (RNG-REQ/ RSP)
(3) SBC-REQ
(4) MS_PreAttachment_Req (Authorization policy)
T1_INE
(5) MS_PreAttachment_Rsp (Authorization policy)
(6) SBC-RSP
T2_INE
(7) MS_PreAttachment_Ack
T3_INE
(8) AuthRelay_EAP_Transfer (EAP Payload: EAP Request/Identity)
(9) PKMv2-RSP/EAP Transfer (EAP Request/ Identity)
(10) PKMv2-REQ/EAP-Transfer (EAP Response/ Identity -NAI)
(11) AuthRelay_EAP_Transfer (EAP Response / Identity-NAI)
(12) EAP Authentication Method (e.g. EAP-PEAP, EAP-TTLS, EAP-TLS, EAP-SIM, EAP-AKA)
(13) EAP Success is indicated and security context is acquired
(14) AuthRelay_EAP_Transfer (EAP Payload, EAP-Success)
(15) PKMv2-RSP/EAP-Transfer (EAP Success)
(16) Key_Change_Directive (AK Context)
T4_INE
(17) Key_Change_Ack
(18) PKMv2-RSP/SA-TEK-Challenge
(19) PKMv2-REQ/SA-TEK-Request
(20) PKMv2-RSP/SA-TEK-Response
(21) PKMv2-REQ/Key-Request
(22) PKMv2-RSP/Key-Reply
(23) REG-REQ
(24) MS_Attachment_Req
T5_INE
(25) MS_Attachment_Rsp
(26) REG-RSP
T6_INE
(27) MS_Attachment_Ack
(29) Connections Establishment (DSA-REQ/ RSP/ ACK)
(28) Data Path Establishment (R6)

Figure 4-54 – MS/AMS Initial Network Entry in BS/ABS(LZone) (Single EAP)

MS/AMS 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/AMS 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/AMS sends an SBC-REQ message starting Basic Capabilities negotiation where MS/AMS and BS/ABS 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/ABS SHALL send *MS_PreAttachment_Req* message to its “default” Authenticator in order to inform it about the new MS/AMS entering the network.

The composition of this *MS_PreAttachment_Req* message is presented in Table 4-44.

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/ABS SHALL assign a value for this R6 context of the MS/AMS and SHALL include R6_Context_ID with this value. Assignment of the value is internal to the BS/ABS. The value SHALL uniquely identify this context of the MS/AMS at this BS/ABS (R6 context). The BS/ABS 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/ABS.

If the resulting MS_PreAttachment_Rsp from the authenticator does not include an R6_Context_ID TLV, the BS/ABS 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/ABS knowledge of the liveliness of the active session, the BS/ABS 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/ABS with *MS_PreAttachment_Rsp* message. The composition of this message is presented in Table 4-45.

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/ABS in the MS_PreAttachment_Req message that initiated this R6 context.

If the MS_PreAttachment_Req message received from the BS/ABS did not include an R6_Context_ID TLV, the authenticator SHALL assume that this BS/ABS 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/AMS.

BS/ABS receiving SBC-REQ sends SBC-RSP message to MS/AMS 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/ABS: 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/ABS to authenticator, there are SBC Context parameters negotiated with authenticator. The BS/ABS should send SBC-RSP message to MS/AMS 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/AMS before the negotiation.

In the case MS/AMS does not receive SBC-RSP, it will retransmit SBC-REQ.

STEP 7

BS/ABS sends *MS_PreAttachment_Ack* message (Table 4-46) to the Authenticator (in ASN/ASN-GW) to confirm that SBC-RSP has been sent to MS/AMS. Note that this does not confirm that MS/AMS has successfully received SBC-RSP.

STEP 8

The Authenticator (in ASN/ASN GW) initiates EAP authentication procedure with MS/AMS. 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/ABS.

The composition of this message is presented in Table 4-47.

STEP 9

The BS/ABS relays the EAP Request/ Identity payload (received in *AR_EAP_Transfer* message) in the PKM-RSP with PKMv2 EAP-Transfer message to the MS.

STEP 10

MS/AMS responds with EAP Response/ Identity message providing NAI. This message is transferred to BS over PKM-REQ with PKMv2 EAP-Transfer message.

STEP 11

BS/ABS 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/AMS. Depending on the realm, EAP payload MAY be forwarded to the MS/AMS 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/AMS and the Authentication server via the Authenticator in ASN/ASNASN-GW. BS/ABS 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 [53]) and forwards the EAP messages received as a payload from the BS/ABS 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/AMS 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/AMS 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/AMS and authentication server).

STEP 13

The Authenticator receives indication about the successful completion of EAP-based authentication, the MS/AMS 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/ABS 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/AMS 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/AMS and an R6_Context exists for this MS/AMS, 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/ABS relays EAP payload (received in *AR_EAP_Transfer* message) to the MS/AMS in PKM-RSP with PKMv2 EAP-Transfer message (not protected by CMAC according to [11]). This message indicates the results of EAP authentication round to the Supplicant in the MS/AMS. Note that the BS/ABS does not relate to the content of EAP Payload – whether it is EAP-Success or EAP-Failure message. The BS/ABS continues waiting for the explicit indication of EAP authentication completion from the Authenticator. MS/AMS is also waiting for PKMv2 SA-TEK-Challengemessage from BS/ABS to proceed with PKMv2 3way handshake.

STEP 16

The Authenticator in ASN/ASN-GW sends *Key_Change_Directive* message to the BS/ABS to indicate completion of the EAP authentication process. The composition of this message is presented in Table 4-12.

This message informs the BS/ABS 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/ABS in the MS_PreAttachment_Req message that initiated this R6 context.

This specification does not define MS/AMS 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/ABS. (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/ABS receiving *Key_Change_Directive* from Authenticator will acknowledge it by *Key_Change_Ack* message.

The BS/ABS 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/ABS 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/ABS and MS/AMS to verify the AK to be used and to establish the Security Association(s) pre-provisioned for the MS/AMS (WiMAX Rel.1 assumes the “default” SA-Descriptor identifying the primary SA to be provisioned in a BS).

The BS/ABS SHALL ensure that PKMv2 3way handshake is indeed successfully completed and the new PMK/AK is enforced by the MS/AMS – i.e., the BS/ABS 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/ABS 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/ABS 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/ABS 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 address). If the BS/ABS 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/ABS for each SA (This step is repeated for each SA).

STEP 23

When PKMv2 3-way handshake is completed, MS/AMS 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/AMS supported capabilities (such as CS capabilities, Mobility parameters and Handover support, etc.).

STEP 24

In the case the BS/ABS detects successful PKMv2 3WHS completion and successfully validates CMAC tuple of REG-REQ message from the MS/AMS, the BS/ABS sends *MS_Attachment_Req* message to the Authenticator including also the MS/AMS REG Context parameters. The composition of this message is presented in Table 4-48.

In case the BS/ABS detects 3-way handshake failure, it SHALL update the Authenticator by sending Key_Change_Cnf message with Key Change Indicator TLV set to indicate “failure”. The Authenticator responds with Key_Change_Ack message to the BS/ABS and initiates MS Network Exit (as described in section 4.5.2).

STEP 25

ASN/ASN GW Authenticator receiving *MS_Attachment_Req* message, responds to BS/ABS with *MS_Attachment_Rsp* message. The composition of this message is presented in Table 4-49.

STEP 26

The BS/ABS sends REG-RSP message to MS/AMS as specified in 6.3.2.3.8 of [11] formatting the appropriate parameters (from BS/ABS policy and/or ASN/ASN GW Authenticator response).

The point in time when REG-RSP is sent is an implementation decision of the BS/ABS: that is, it may be sent before or after performing the *MS_Attachment_Req* and *MS_Attachment_Rsp* exchange with the ASN/ASN GW Authenticator.

If the REG Context is included in MS_Attachment_Req message from BS/ABS to authenticator, there are REG Context parameters negotiated with authenticator. The BS/ABS SHALL send REG-RSP message to MS/AMS 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/AMS before the negotiation. In case the MS/AMS does not receive REG-RSP, it will retransmit REG-REQ.

STEP 27

The BS/ABS sends *MS_Attachment_Ack* message (Table 4-50) 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/AMS. 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/ABS 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/AMS.

Note: After the creation of ISF, and as long as the IP session (s) is/are not established for the MS/AMS, it is operator/network policy when to initiate Network exit for the MS/AMS as specified in section 4.5.2.

4.5.1.1.2 Network entry in ABS(Mzone)

Figure 4-55 describes normative procedures for an initial AMS network entry focusing on AMS-to-Network EAP authentication process (single EAP) and AMS 802.16m registration.

The BS/ABS 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.

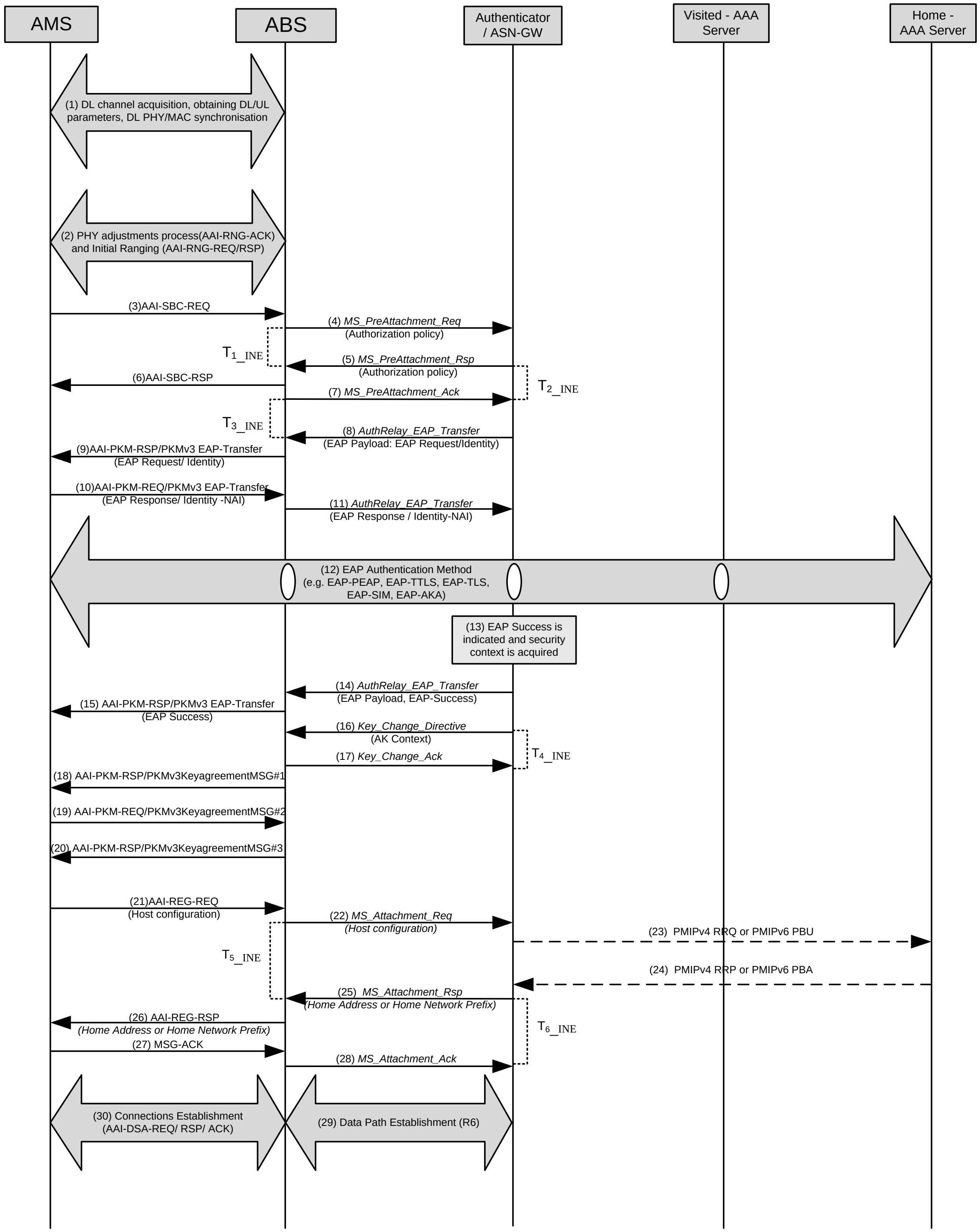

AMS
ABS
Authenticator / ASN-GW
Visited - AAA Server
Home - AAA Server
(1) DL channel acquisition, obtaining DL/UL parameters, DL PHY/MAC synchronisation
(2) PHY adjustments process(AAI-RNG-ACK) and Initial Ranging (AAI-RNG-REQ/RSP)
(3)AAI-SBC-REQ
(4) MS_PreAttachment_Req (Authorization policy)
T1_INE
(5) MS_PreAttachment_Rsp (Authorization policy)
(6)AAI-SBC-RSP
(7) MS_PreAttachment_Ack
T2_INE
T3_INE
(8) AuthRelay_EAP_Transfer (EAP Payload: EAP Request/Identity)
(9)AAI-PKM-RSP/PKMv3 EAP-Transfer (EAP Request/ Identity)
(10)AAI-PKM-REQ/PKMv3 EAP-Transfer (EAP Response/ Identity -NAI)
(11) AuthRelay_EAP_Transfer (EAP Response / Identity-NAI)
(12) EAP Authentication Method (e.g. EAP-PEAP, EAP-TTLS, EAP-TLS, EAP-SIM, EAP-AKA)
(13) EAP Success is indicated and security context is acquired
(14) AuthRelay_EAP_Transfer (EAP Payload, EAP-Success)
(15) AAI-PKM-RSP/PKMv3 EAP-Transfer (EAP Success)
(16) Key_Change_Directive (AK Context)
(17) Key_Change_Ack
T4_INE
(18) AAI-PKM-RSP/PKMv3KeyagreementMSG#1
(19) AAI-PKM-REQ/PKMv3KeyagreementMSG#2
(20) AAI-PKM-RSP/PKMv3KeyagreementMSG#3
(21)AAI-REG-REQ (Host configuration)
(22) MS_Attachment_Req (Host configuration)
(23) PMIPv4 RRQ or PMIPv6 PBU
T5_INE
(24) PMIPv4 RRP or PMIPv6 PBA
(25) MS_Attachment_Rsp (Home Address or Home Network Prefix)
(26) AAI-REG-RSP (Home Address or Home Network Prefix)
T6_INE
(27) MSG-ACK
(28) MS_Attachment_Ack
(30) Connections Establishment (AAI-DSA-REQ/ RSP/ ACK)
(29) Data Path Establishment (R6)

Figure 4-55 – AMS Initial Network Entry in ABS(MZone) (Single EAP)

802.16m AMS Network Entry starts:

STEP 1

DL channel acquisition, MAC synchronization and obtaining UL channel parameters.

STEP 2

Initial Ranging round trips – AAI-RNG-REQ/AAI-RNG-RSP message exchange. The AMS performing initial network entry will perform CDMA ranging and after that will send AAI-RNG-REQ message indicating that it performs initial entry. When the MSID privacy is applied, AAI-RNG-REQ message carries MSID*, but not AMS MAC address. AMS MAC address is delivered from AMS by AAI-REG-REQ in step 21. For location privacy, a temporary STID(TSTID) SHALL be assigned to AMS by AAI-RNG-RSP, which is used until an STID is assigned successfully to the AMS through encrypted AAI-REG-RSP in stage 28.

STEP 3

AMS sends an AAI-SBC-REQ message starting Basic Capabilities negotiation where AMS and ABS among other parameters negotiate the PKM protocol version, Authorization Policy and Message Authentication Code mode (in ABS(MZone) PKM protocol version and Message Authentication Code mode are not negotiated, but PKMv3 and CMAC are used mandatorily). AMS MAY also include an attribute Visited NSP ID in AAI-SBC-REQ to request the realm of the selected NSP.

STEP 4

The ABS SHALL send *MS_PreAttachment_Req* message to its "default" Authenticator in order to inform it about the new AMS entering the network.

The composition of this *MS_PreAttachment_Req* message is presented in Table 4-44.

The ABS SHALL assign a value for this R6 context of the AMS and SHALL include R6_Context_ID with this value. Assignment of the value is internal to the ABS. The value SHALL uniquely identify this context of the AMS at this ABS (R6 context). The ABS 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 ABS.

If the resulting MS_PreAttachment_Rsp from the authenticator does not include an R6_Context_ID TLV, the ABS 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 ABS knowledge of the liveliness of the active session, the ABS MAY ignore the AAI-RNG-REQ of the new MS entry with the MS using the same MAC address/MSID*.

STEP 5

Authenticator in the ASN/ASN-GW receiving *MS_PreAttachment_Req* creates a new context block related to this MSID/MSID* and responds to ABS with *MS_PreAttachment_Rsp* message. The composition of this message is presented in .Table 4-45

STEP 6

The authenticator SHALL include R6_Context_ID in MS_PreAttachment_Rsp with the value set to the same value received from the ABS in the MS_PreAttachment_Req message that initiated this R6 context.

If the MS_PreAttachment_Req message received from the ABS did not include an R6_Context_ID TLV, the authenticator SHALL assume that this ABS does not support R6_Context_ID and SHALL not include R6_Context_ID in any subsequent R6 message for this R6 context of the AMS.

ABS receiving AAI-SBC-REQ sends AAI-SBC-RSP message to AMS enforcing the authentication framework policy (PKMv3, single EAP, CMAC mode). If AMS includes an attribute Visited NSP ID in AAI-SBC-REQ, ABS SHALL include an attribute Visited NSP Realm in AAI-SBC-RSP.

The point in time when AAI-SBC-RSP is sent is an implementation decision of the ABS: 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 ABS to authenticator, there are SBC Context parameters negotiated with authenticator. The ABS should send AAI-SBC-RSP message to AMS after performing the *MS_PreAttachment_Req* and *MS_PreAttachment_Rsp* exchange with the ASN/ASN GW Authenticator. Otherwise, the AAI-SBC-RSP may be sent to AMS before the negotiation.

In the case AMS does not receive AAI-SBC-RSP, it will retransmit AAI-SBC-REQ.

STEP 7

ABS sends *MS_PreAttachment_Ack* message to the Authenticator (in ASN/ASN-GW) to confirm that AAI-SBC-RSP has been sent to AMS. Note that this does not confirm that AMS has successfully received AAI-SBC-RSP.

STEP 8

The Authenticator (in ASN/ASN GW) initiates EAP authentication procedure with AMS. 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 ABS.

The composition of this message is presented in Table 4-47.

STEP 9

The ABS relays the EAP Request/ Identity payload (received in *AR_EAP_Transfer* message) in the AAI-PKM-RSP withPKMv3 EAP-Transfer message to the AMS.

STEP 10

AMS responds with EAP Response/ Identity message providing NAI. This message is transferred to ABS over AAI-PKM-REQ withPKMv3 EAP-Transfer message.

STEP 11

ABS relays EAP payload received in PKMv3 EAP-Transfer to the Authenticator over Authentication Relay protocol (*AR_EAP_Transfer* message).

STEP 12

The Authenticator analyses the NAI provided by the AMS Depending on the realm, EAP payload MAY be forwarded to the AMS' 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 AMS and the Authentication server via the Authenticator in ASN/ASNASN-GW. ABS provides "relay" of EAP payload from PKMv3 EAP-Transfer messages to *AR_EAP_Transfer* and vice versa. The Authenticator in ASN/ASN-GW acts in pass through mode (as described in [53]) and forwards the EAP messages received as a payload from the ABS 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 AMS 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 AMS 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 AMS and authentication server).

STEP 13

The Authenticator receives indication about the successful completion of EAP-based authentication, the AMS 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 ABS as EAP Payload TLV in *AR_EAP_Transfer* message.

In the case of EAP-Success, if the NAS can confirm that the newly authenticated AMS 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 AMS and an R6_Context exists for this AMS, the NAS SHALL include the R6_Context_ID value of this R6 Context in any *NetExit_State_Change_Req/Rsp* message.

STEP 15

The ABS relays EAP payload (received in *AR_EAP_Transfer* message) to the AMS in AAI-PKM-RSP with PKMv3 EAP-Transfer message (not protected by CMAC according to [11]). This message indicates the results of EAP authentication round to the Supplicant in the AMS. Note that the ABS does not relate to the content of EAP Payload – whether it is EAP-Success or EAP-Failure message. The ABS continues waiting for the explicit indication of EAP authentication completion from the Authenticator. AMS is also waiting for PKMv3 Key agreement MSG#1 message from ABS to proceed with PKMv3 Key agreement 3way handshake.

STEP 16

The Authenticator in ASN/ASN-GW sends *Key_Change_Directive* message to the ABS to indicate completion of the EAP authentication process. The composition of this message is presented in Table 4-12:

This message informs the ABS that it SHOULD proceed with PKMv3 Key agreement 3way 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 ABS in the MS_PreAttachment_Req message that initiated this R6 context.

This specification does not define AMS 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 an ABS. (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

ABS receiving *Key_Change_Directive* from Authenticator will acknowledge it by *Key_Change_Ack* message.

The ABS 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 ABS 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

PKMv3 Key agreement 3way handshake(Key agreement MSG #1/#2/#3 exchange) is conducted between ABS and AMS to verify the AK to be used and to establish the Security Association(s) pre-provisioned for the AMS (WiMAX Rel.2 defines the primary SA as security association applying AES-CCM encryption method).

The ABS SHALL ensure that PKMv3 Key agreement 3way handshake is indeed successfully completed and the new PMK/AK is enforced by the AMS – i.e., the ABS should receive and verify a MAC management message(i.e. in step 21 AAI-REG-REQ) from the AMS encrypted by TEK derived from the new AK.

When ABS recognizes the completion of PKMv3 Key agreement 3way handshake (success or failure), it SHALL indicate this event to Authenticator. This indication is described in the step 22.

After receiving successfully AAI-REG-REQ in the step21 following the PKMv3 key agreement 3way handshake, that the MAC address of the new entry is already part of another authenticated MS context and the latter AMS is using a different authenticator than the new entry, the ABS SHALL initiate network exit for the latter AMS (if the same authenticator is used, the authenticator is in charge of triggering network exit for any overlapping MAC address).

If the ABS 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

When PKMv3 key agreement 3way handshake is completed, AMS proceeds with 802.16m Registration procedure by sending AAI-REG-REQ message. This message will carry the AMS supported capabilities (such as CS capabilities etc.).

AMS transmits AMS MAC address by encrypted AAI-REG-REQ and if attached to FIAA compliant ASN-GW, for Fast IP Address Allocation(FIAA), the AMS MAY include either Host-Configuration-Capability-Indicator or Requested-Host-Configurations IE in the AAI-REG-REQ to request configuration using FIAA procedure.

STEP 22

In the case the ABS detects successful PKMv3 3WHS completion and successfully validates AAI-REG-REQ message from the AMS, the ABS sends *MS_Attachment_Req* message to the Authenticator including also the MS REG Context parameters.

For Fast IP Address Allocation(FIAA) ABS forwards the received Host-Configuration-Capability-Indicator or Requested-Host-Configurations IE to the AR (FIAA compliant ASN-GW) via MS_Attachment_Req.

The composition of this message is presented in Table 4-58 – MS_Attachment_Req from BS to Authenticator

:

In case the ABS detects 3-way handshake failure, it SHALL update the Authenticator by sending Key_Change_Cnf message with Key Change Indicator TLV set to indicate "failure". The Authenticator responds with Key_Change_Ack message to the ABS and initiates MS Network Exit (as described in section 4.5.2).

STEP 23

The authenticator in ASN/ASN-GW requests an IPv4 Home address or IPv6 Home Network Prefix for FIAA. If FIAA is not supported, the STEP 23 and 24 SHALL be skipped.

STEP 24

The authenticator in ASN/ASN-GW obtains an IPv4 Home address or IPv6 Home Network Prefix for FIAA. If FIAA is not supported, the STEP 23 and 24 SHALL be skipped.

STEP 25

ASN/ASN GW Authenticator receiving *MS_Attachment_Req* message and obtaining, if FIAA is supported, IPv4 Host Address/IPv6 Home Network Prefix, responds to ABS with *MS_Attachment_Rsp* message.

For FIAA procedure AR(ASN-GW) responds with MS_Attachment_Rsp that carries IPv4 Host Address/IPv6 Home Network Prefix and Additional-Host-Configurations IEs, if it is configured to do so based on the operator policy. ABS forwards the received IE(s) to the AMS via AAI_REG-RSP in STEP 26, and sends back the acknowledgement to AR via MS_Attachment_Ack in STEP 27.

The composition of this message is presented in Table 4-59 – MS_Attachment_Rsp from Authenticator to BS

:

STEP 26

The ABS sends AAI-REG-RSP message to AMS formatting the appropriate parameters (from ABS policy and/or ASN/ASN GW Authenticator response. If FIAA is applied, IPv4 Host Address/IPv6 Home Network Prefix is included in AAI-REG-RSP).

For location privacy the ABS SHALL assign an STID to AMS by encrypted AAI-RNG-RSP so that the TSTID used is released and replaced with STID.

The point in time when AAI-REG-RSP is sent is an implementation decision of the ABS: that is, it may be sent before or after performing the *MS_Attachment_Req* and *MS_Attachment_Rsp* exchange with the ASN/ASN GW Authenticator.

If the REG Context is included in MS_Attachment_Req message from ABS to authenticator, there are REG Context parameters negotiated with authenticator. The ABS SHALL send AAI-REG-RSP message to AMS after performing the *MS_Attachment_Req* and *MS_Attachment_Rsp* exchange with the ASN/ASN GW Authenticator. Otherwise, the AAI-REG-RSP may be sent to AMS before the negotiation. In case the AMS does not receive AAI-REG-RSP, it will retransmit AAI-REG-REQ.

STEP 27

AMS responds with MSG-ACK.

STEP 28

The ABS 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 AAI-REG-RSP message has been sent to AMS. This message serves as a trigger to the ASN/ASN GW Authenticator to initiate the pre-provisioned service flows establishment procedure. In the case of a network entry through ABS(MZone) attached to a Release 2 ASN-GW a default service flow(DSF) is established.

STEP 29, 30

ASN/ASN-GW triggers SFA to create the Initial service flow (ISF) and optionally other pre-provisioned service flows. The ABS 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 AMS.

Note: After the creation of ISF, and as long as the IP session (s) is/are not established for the AMS, it is operator/network policy when to initiate Network exit for the AMS as specified in section 4.5.2.

4.5.1.1.3 Message composition

Table 4-44 – MS_PreAttachment_Req from BS/ABS to Authenticator

TLV	Reference	M/O	Notes	Applicability
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier	1,2,3
MS Info	5.3.2.103	M	Contains MS/AMS-related context in the nested IEs.	1,2,3
MSID	5.3.2.102	O	See 3.6.	3
>MS Security History	5.3.2.108	M		1,2,3
>>Authorization Policy Support	5.3.2.21	M	Identifies the MS authorization policy.	1,2,3
>SBC Context	5.3.2.174	O	802.16e/16m related MS session context.	1,2,3
>>Subscriber Transition Gaps	5.3.2.316	O		1,2
>>Maximum Transmit Power	5.3.2.317	O		1,2,3
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	O		1,2
>>PKM Flow Control	5.3.2.319	O		1,2
>>Maximum Number of Supported Security Associations	5.3.2.320	O		1,2
>>Security Negotiation Parameters	5.3.2.321	O		1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2
>>>Authorization Policy Support	5.3.2.21	CM		1,2
>>>MAC Mode	5.3.2.322	CM		1,2
>>>PN Window Size	5.3.2.324	CM		1,2
>>Association type support	5.3.2.465	O		1,2
>>Extended Subheader Capability	5.3.2.325	O		1,2

TLV	Reference	M/O	Notes	Applicability
>>HO Trigger Metric Support	5.3.2.326	O		1,2 (in case of applicability 3 and 4, this TLV is moved to REG context)
>>Current Transmit Power	5.3.2.327	O		1,2
>>OFDMA SS FFT Sizes	5.3.2.328	O		1,2,3
>>OFDMA SS demodulator	5.3.2.329	O		1,2
>>OFDMA SS modulator	5.3.2.330	O		1,2
>>The number of UL HARQ Channel	5.3.2.331	O		1,2
>>OFDMA SS Permutation support	5.3.2.332	O		1,2
>>OFDMA SS CINR Measurement Capability	5.3.2.333	O		1,2
>>The number of DL HARQ Channels	5.3.2.334	O		1,2
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	O		1,2
>>OFDMA SS Uplink Power Control Support	5.3.2.336	O		1,2
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	O		1,2
>>OFDMA MAP Capability	5.3.2.338	O		1,2
>>Uplink Control Channel Support	5.3.2.339	O		1,2
>>OFDMA MS CSIT Capability	5.3.2.340	O		1,2
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	O		1,2
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	O		1,2
>>OFDMA SS modulator for MIMO Support	5.3.2.343	O		1,2
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	O		1,2
>>CAPABILITY_INDEX	5.3.2.503	O		3

TLV	Reference	M/O	Notes	Applicability
>>DEVICE_CLASS	5.3.2.504	O		3
>>CLC Request	5.3.2.505	O		3
>>Long TTI for DL	5.3.2.506	O		3
>>UL sounding	5.3.2.507	O		3
>>OL Region	5.3.2.508	O		3
>>DL resource metric for FFR	5.3.2.509	O		3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O		3
>>DL MIMO mode	5.3.2.512	O		3
>>feedback support for DL	5.3.2.513	O		3
>>Subband assignment A-MAP IE support	5.3.2.514	O		3
>>DL pilot pattern for MU MIMO	5.3.2.515	O		3
>>Number of Tx antenna of AMS	5.3.2.516	O		3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O		3
>>UL pilot pattern for MU MIMO	5.3.2.519	O		3
>>UL MIMO mode	5.3.2.520	O		3
>>Modulation scheme	5.3.2.521	O		3
>>UL HARQ buffering capability	5.3.2.522	O		3
>>DL HARQ buffering capability	5.3.2.523	O		3
>>AMS DL processing capability per sub-frame	5.3.2.524	O		3
>>AMS UL processing capability per sub-frame	5.3.2.525	O		3
>>FFT size(2048/1024/512)	5.3.2.526	O		3
>>Authorization policy support	5.3.2.21	O		3
>>Inter-RAT Operation Mode	5.3.2.527	O		3
>>Supported Inter-RAT type	5.3.2.528	O		3
>>MIH Capability Supported	5.3.2.529	O		3

TLV	Reference	M/O	Notes	Applicability
>>MS MAC Version	5.3.2.106	O	MS/AMS reported MAC Version. Note that MS/AMS MAC Version included in TLV-148 is no longer used for an indication of MS/AMS capability of ND&S.	1,2,3
BS Info	5.3.2.26	M	Contains relevant Serving BS/ABS context in the nested IEs.	1,2,3
> BS ID	5.3.2.25	M	Serving BS ID.	1,2,3
>BS Location	5.3.2.425	O	Location info of the serving BS/ABS which may be described as Lat/Long/Sector/Carrier information of BS/ABS. NAS may pass this info to H-AAA which can use it to authorize stationary access services.	1,2,3
> IP Address of Requesting BS	5.3.2.458	M	IP Address of requesting BS/ABS.	1,2,3

Table 4-45 – MS_PreAttachment_Rsp from Authenticator to BS/ABS

TLV	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/AMS. When this TLV is presented, BS/ABS 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.

Table 4-46 – MS_PreAttachment_Ack from BS/ABS to Authenticator

TLV	Reference	M/O	Notes
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	
Failure Indication	5.3.2.69	O	TC bit SHALL be set to 1.

Table 4-47 – AR_EAP_Transfer from Authenticator to BS/ABS (EAP initiation)

TLV	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.
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	

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/ABS in the MS_PreAttachment_Req message that initiated this R6 context.

Table 4-48 – MS_Attachment_Req from BS/ABS to Authenticator

TLV	Reference	M/O	Notes	Applicability
MS Info	5.3.2.103	M	Contains MS/AMS-related context in the nested IEs.	1,2
> SF Info	5.3.2.185	O	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.	1,2,3
>> Data Path Info	5.3.2.45	CM	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.	1,2,3

TLV	Reference	M/O	Notes	Applicabili ty
>>> Data Path ID	5.3.2.44	CM	Specifies the data path for default service flow.	1,2,3
>>> Tunnel Endpoint	5.3.2.194	O		1,2,3
>AMS MAC address	5.3.2.102	M		3
> REG Context	5.3.2.144	O	SHALL be included if it is received from MS/AMS in REG-REQ/AAI-REG-REQ and as supported by the BS/ABS.	1,2
>>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. For 16m the value may be set by 13.	1,2
>>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. For 16m the value may be set by 13.	1,2
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	O	This TLV SHALL be included if REG Context is included in the transmitted message. It is named as 'CS type support' in 16m.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ARQ is supported).	1,2
>>DSx Flow Control	5.3.2.294	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>Maximum MAC Data per Frame Support	5.3.2.296	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

TLV	Reference	M/O	Notes	Applicability
>>>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. For 16m the value may be set by 0(i.e. unlimited) or predefined value.	1,2
>>>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. For 16m the value may be set by 0(i.e. unlimited) or predefined value.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. packing supported).	1,2
>>MAC ertPS Support	5.3.2.300	O	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ertPS supported).	1,2
>>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. For 16m the value may be set by a predefined value.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2

TLV	Reference	M/O	Notes	Applicability
>>Idle Mode Timeout	5.3.2.268	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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. For 16m the value may be set by a predefined value.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>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. For 16m the value may be set by a predefined value.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O		3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O		3
>>Multicarrier capabilities	5.3.2.485	O		3

TLV	Reference	M/O	Notes	Applicability
>>Zone Switch Mode Support	5.3.2.486	O		3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O		3
>>Interference mitigation supported	5.3.2.488	O		3
>>E-MBS capabilities	5.3.2.489	O		3
>>Channel BW and Cyclic prefix	5.3.2.490	O		3
>>frame configuration to support legacy R1.0	5.3.2.491	O		3
>>Persistent Allocation support	5.3.2.492	O		3
>>Group Resource Allocation support	5.3.2.493	O		3
>>Co-located coexistence capability support	5.3.2.494	O		3
>>HO Trigger Metric Support	5.3.2.326	O		3
>>EBB Handover support	5.3.2.495	O		3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O		3
>>Capability for sounding antenna switching support	5.3.2.497	O		3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O		3
>>ROHC support	5.3.2.499	O		3
>>Host-Configuration-Capability-Indicator	5.3.2.536	M		3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O		3
>Requested-Host-Configurations	5.3.2.537	O	This TLV may be included only when Host-Configuration-Capability-Indicator is set by 0b1.	3
BS Info	5.3.2.26	M		1,2,3
> BS ID	5.3.2.25	M	Serving BS ID	1,2,3
>Reattachment Zone	5.3.2.424	O	Included if configured at BS/ABS. 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.	1,2,3

Table 4-49 – MS_Attachment_Rsp from Authenticator to BS/ABS

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3
MS Info	5.3.2.103	O	Contains MS/AMS-related context in the nested IEs.	1,2,3
> SF Info	5.3.2.185	O	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.	1,2,3
>> Data Path Info	5.3.2.45	CM	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.	1,2,3
>>> Data Path ID	5.3.2.44	CM	Specifies the data path for default service flow.	1,2,3
>>> Tunnel Endpoint	5.3.2.194	O		1,2,3
>CRID	5.3.2.475	M	The CRID that was allocated for the AMS by the DCR Controller. This TLV does not exist only when the responding Authenticator does not have a DCR Controller (Legacy ASN-GW)	3
> REG Context	5.3.2.144	O	Identifies the MS REG Context parameters as enforced by the Authenticator. SHALL be included if it is include in the MS_Attachment_Req message.	1,2,3
>>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. For 16m the value may be set by 13.	1,2
>>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. For 16m the value may be set by 13.	1,2
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	O	This TLV SHALL be included if REG Context is included in the transmitted message. It is named as ‘CS type support’ in 16m.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3

TLV	Reference	M/O	Notes	Applicability
>>PHS Support	5.3.2.292	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ARQ is supported).	1,2
>>DSx Flow Control	5.3.2.294	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>Total Number of Provisioned Service Flows	5.3.2.295	O		1,2
>>Maximum MAC Data per Frame Support	5.3.2.296	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>>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. For 16m the value may be set by 0(i.e. unlimited) or predefined value.	1,2
>>>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. For 16m the value may be set by 0(i.e. unlimited) or predefined value.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. packing supported).	1,2
>>MAC ertPS Support	5.3.2.300	O	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ertPS supported).	1,2

TLV	Reference	M/O	Notes	Applicability
>>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. For 16m the value may be set by a predefined value.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>Idle Mode Timeout	5.3.2.268	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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. For 16m the value may be set by a predefined value.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>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. For 16m the value may be set by a predefined value.	1,2

TLV	Reference	M/O	Notes	Applicability
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by a predefined value.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O		3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O		3
>>Multicarrier capabilities	5.3.2.485	O		3
>>Zone Switch Mode Support	5.3.2.486	O		3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O		3
>>Interference mitigation supported	5.3.2.488	O		3
>>E-MBS capabilities	5.3.2.489	O		3
>>Channel BW and Cyclic prefix	5.3.2.490	O		3
>>frame configuration to support legacy R1.0	5.3.2.491	O		3
>>Persistent Allocation support	5.3.2.492	O		3
>>Group Resource Allocation support	5.3.2.493	O		3
>>Co-located coexistence capability support	5.3.2.494	O		3
>>HO Trigger Metric Support	5.3.2.326	O		3
>>EBB Handover support	5.3.2.495	O		3

TLV	Reference	M/O	Notes	Applicability
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O		3
>>Capability for sounding antenna switching support	5.3.2.497	O		3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O		3
>>ROHC support	5.3.2.499	O		3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O		3
>IPv4-Host-Address IE	5.3.2.476	CM	If FIAA is supported either this TLV or IPv6-Home-Network-Prefix IE SHALL be included.	3
>IPv6-Home-Network-Prefix IE	5.3.2.477	CM	If FIAA is supported either this TLV or IPv4-Host-Address IE SHALL be included.	3
>Additional-Host-Configurations IE	5.3.2.478	O	If FIAA is supported, this TLV may be included.	3
>CS specification for default service flow	5.3.2.501	M		3
>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.	1,2,3
>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).	1,2,3
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M		1,2,3

Table 4-50 – MS_Attachment_Ack from BS/ABS to Authenticator

TLV	Reference	M/O	Notes
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	
Failure Indication	5.3.2.69	O	

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/ABS 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/ABS 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/ABS 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 4-51 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-51 – 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
T_{5_INE}	TBD		TBD
T_{6_INE}	TBD		TBD

4.5.1.2.2 Handling Error Conditions

Table 4-52 lists the behavior for various error conditions during Initial Network Entry:

Table 4-52 – Initial Network Entry – Handling Error Conditions

	Failure Case	Action
1	Auth failure at the Authenticator.	The authenticator initiates Network Exit procedure by sending NetExit_MS_State_Change_Req with Action Code set to 0xfffe which indicates initial authentication failure as described in the section 4.5.2.1.2.4.
2	*MS_PreAttachment_Req* or *MS_Attachment_Req* messages not understood by the Authenticator (decode error, corrupted packet etc.).	Send *MS_PreAttachment_Rsp* (or *MS_Attachment_Rsp* correspondingly) with Failure Indication TLV.
3	*MS_PreAttachment_Rsp* or *MS_PreAttachment*_Ack messages are not understood by the Authenticator or BS/ABS (decode error, corrupted packet etc.).	Discard the message, no response generated.
4	Internal error at the Authenticator or BS/ABS – need to abort the call.	Initiate MS Network Exit (as described in the section 4.5.2.1.2.4).
5	MS/AMS dropped call at the BS/ABS during call setup.	Initiate to the peer entity using procedure described in the MS Network Exit section 4.5.2.1.2.4.
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 *Path_Dereg_Req*.
8	*Path_Dereg_Req* received for a MS/AMS or Data Path that does not exist.	Respond with *Path_Dereg_Rsp* with Success so that the peer does not retry.
9	BS/ABS receives SBC-REQ/AAI-SBC-REQ message retransmission from the MS/AMS (SBC-REQ/AAI-SBC-REQ retransmission as a result of timer expiry in the MS/AMS or SBC-RSP/AAI-SBC-RSP message loss).	BS/ABS resends *MS_PreAttachment_Req* message for the same MSID with a new Transaction ID value. Authenticator should restart the transaction - respond with *MS_PreAttachment_Rsp* and reset T_{2_INE} timer.
10	BS/ABS receives REG-REQ/AAI-REG-REQ message retransmission from the MS/AMS (REG-REQ/AAI-REG-REQ retransmission as a result of timer expiry in the MS/AMS or REG-RSP/AAI-REG-RSP message loss).	BS/ABS resends *MS_Attachment_Req* message for the same MSID with a new Transaction ID value. Authenticator should restart the transaction - respond with *MS_Attachment_Rsp* and reset T_{6_INE} timer.
11	BS/ABS detects PKMv2 3way handshake failure or PKMv3 key agreement 3way handshake failure for any reason.	BS/ABS sends *Key_Change_Cnf* message with Key Change Indicator TLV set to indicate "failure". Authenticator responds with *Key_Change_Ack* message and initiates MS Network Exit (as described in the section 4.5.2.1.2.4).

4.5.1.2.3 Timer Expiry

Table 4-53 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 4-53.

Table 4-53 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
T_{1_INE}	BS/ABS	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T_{2_INE}	Authenticator	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T_{3_INE}	BS/ABS	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T_{4_INE}	Authenticator	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T_{5_INE}	BS/ABS	Initiate MS Network Exit (as described in section 4.5.2.1.1).
T_{6_INE}	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/AMS 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 MS/AMSs 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/AMS but may for example be launched by a MS/AMS that was reset while being in idle mode. In this case the network may not be aware of the real MS/AMS status and may still consider the idle MS/AMS as being a valid session. Hence, the MS/AMS has to be allowed a new initial network entry after successful authentication and authorization.

A MS/AMS 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. However, when MSID privacy is applied, network exit will be triggered for the already existing WiMAX session with the same MAC address after receiving AMS MAC address from AMS by AAI-REG-REQ message. This is to allow a MS/AMS to re-enter the network in case of any fatal state loss at the MS/AMS 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/ABS 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/AMS to negatively impact or terminate ongoing WiMAX sessions of legitimate MSs through MAC address spoofing, without proper authentication based on a valid subscription. On the contrary, for any misbehaving or malfunctioning MS/AMS 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/AMS MAC addresses is to enforce device authentication during initial network entry. When required to perform device authentication based on the device certificate, the MS/AMS 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/ABS knowledge of the liveliness of the active session, the BS/ABS MAY ignore the RNG-REQ/AAI-RNG-REQ of the new MS/AMS entry with the MS/AMS 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 ASN-GW Selection and R6 Flex Support

When an MS/AMS enters a network; during the INE process, the serving BS/ABS needs to select an ASN-GW for this MS/AMS. The selected ASN-GW SHALL be within the same ASN that the BS/ABS belongs to. The selected ASN-GW may in turn select another ASN-GW for the MS/AMS, based on load information of the other ASN-GWs in the ASN or some other algorithm. The process for this is described below.

The BS/ABS mechanism of load distribution inside an "ASN-GW cluster" is out of the specification scope. E.g. this mechanism may be based on a round-robin distribution among ASN-GWs of the same "ASN-GW cluster". If the BS/ABS is associated with multiple "clusters", the distribution algorithm may be based on a more complicated scheme, e.g. each "cluster" may be provided with a "metric" – example: the relative priority of the "cluster". In this case, the BS/ABS may use "load distribution" inside of the top priority cluster and switch-over to the lower priority cluster only when there are no ASN-GWs available in the higher priority cluster.

The load distribution between the ASN-GWs of the same cluster may be impacted also by the "capacity/ load factor" of the ASN-GW in the cluster. The "capacity/ load factor" reflects the real-time load or relative capacity of the particular ASN-GW. The BS/ABS distribution mechanism in this case may be based on "weighted round-robin" algorithm.

The "capacity/ load factor" and "metric" parameters for ASN-GW load distribution are subject of the internal BS/ABS implementation and are out of the specification scope.

A BS/ABS may be aware of the operational status of the ASN-GW status (i.e. Active, Out of Service etc) by using R6 per-MS/AMS transactions (e.g. transactions failure or explicit rejections) or by using MS/AMS-independent Keep-alive mechanism.

During MS/AMS INE, the BS/ABS sends MS Pre-attachment Req message to one of the ASN-GWs in the cluster. How the BS/ABS chooses this ASN-GW is out of scope of the specification and is specific to the algorithms and implementation within the BS/ABS. If the chosen ASN-GW (as Authenticator or Anchor GW) can support the incoming request, it responds back to the BS/ABS with a positive MS Pre-attachment Rsp message.

If the chosen ASN-GW cannot support the incoming request from the BS/ABS, due to overloading and/or other conditions, it sends MS Pre-attachment Rsp message to a BS/ABS with either

a) Failure Indication TLV (5.3.2.69) set to indicate "no resources".

Or

b) Authenticator ID TLV (5.3.2.19) containing the IP address of a "redirected" ASN-GW that has resources to support the INE request by the BS/ABS.

In case (a), the BS/ABS may try the next ASN-GW in the "cluster", and so on, until one of the ASN-GWs responds positively. In order to neutralize the MS/AMS SBC-REQ retransmission timer (Wait for SBC-RSP timeout or Wait for AAI-SBC-RSP timeout), the BS/ABS may respond back to MS/AMS with "early" SBC-RSP /AAI-SBC-RSP message (without waiting for the positive MS Pre-attachment RSP) using cached authorization policy. Note that the BS/ABS may continue with the subsequent ASN-GW selection procedure until it succeeds or until an INE Failure occurs, limited by MS/AMS waiting for the successful authentication completion (relatively long timer).

In case (b), the BS/ABS will:

- update the Authenticator Identity (Authenticator ID) in the MS context and assign it to the Authenticator ID provided in the MS Pre-attachment Rsp message,
- send a MS Pre-attachment Ack message to the original ASN-GW, and
- wait for INE continuation from the new ASN-GW (the "redirected" ASN-GW) – the next expected transaction is EAP-Request/ Identity (Authentication Relay EAP-Transfer) message sent by the "redirected" ASN-GW.

In case (b), the originally selected ASN-GW triggers the "redirected" ASN-GW to start EAP authentication session with the MS/AMS via the Serving BS/ABS. The "redirected" ASN-GW starts EAP authentication process by sending R6 Authentication Relay EAP-Transfer message with EAP-Request/ Identity content to the BS/ABS.

From this point on, the INE procedure continues as usual with the "redirected" ASN-GW and this ASN-GW becomes the assigned Authenticator of the MS/AMS.

The communications between the ASN-GWs during ASN-GW re-direction for parameters such as availability status, capacity, real-time load factor, etc. are out of the scope of this specification.

4.5.1.3.1 Case a - ASN-GW Selected by BS/ABS

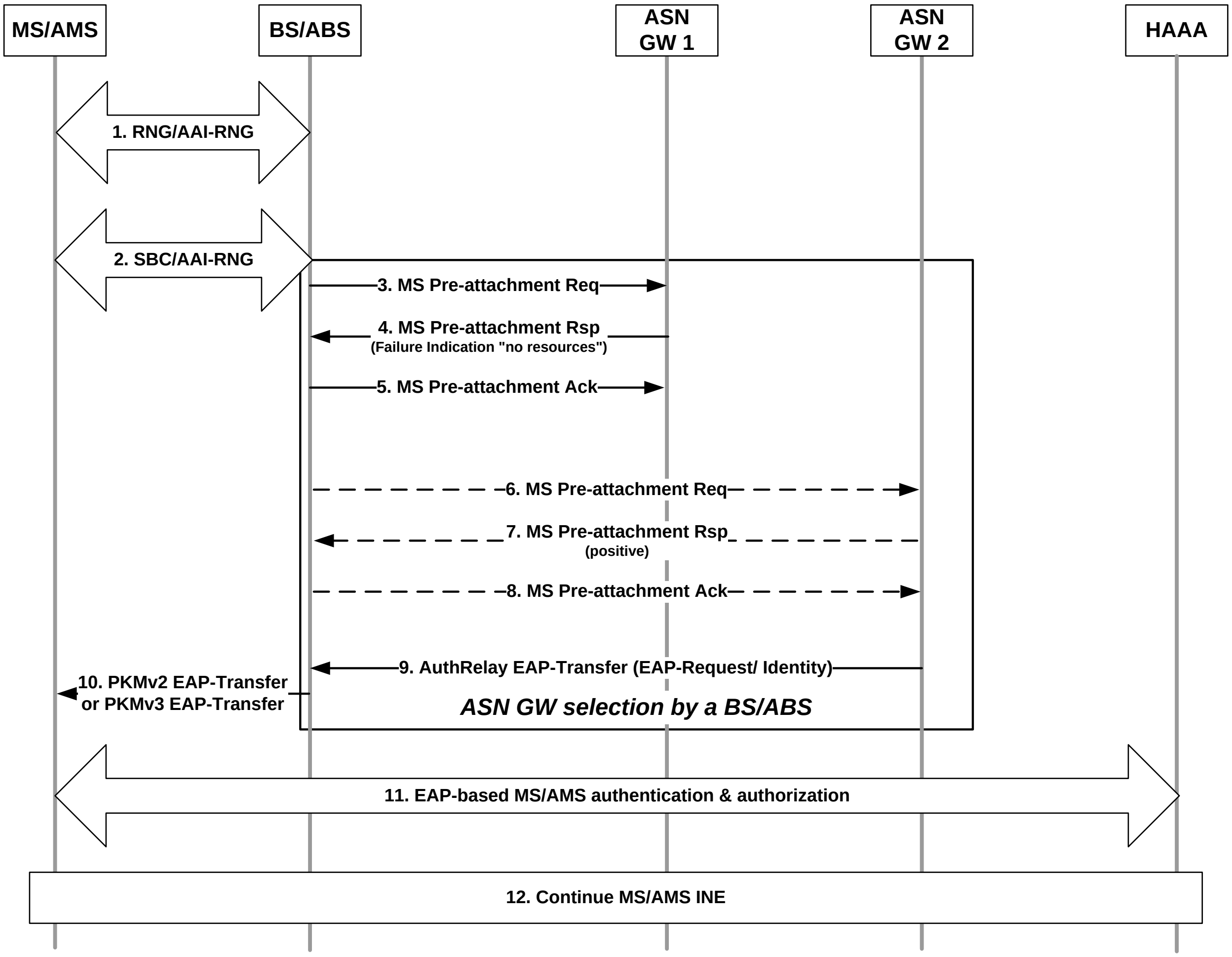


Figure 4-56 – ASN-GW selection by a BS/ABS during MS/AMS INE

1. MS/AMS starts INE process with the BS/ABS and performs MAC Ranging.

2. After RNG/AAI-RNG is complete, MS performs SBC/AAI-SBC transaction with the BS/ABS.

3. The BS/ABS receiving SBC-REQ/AAI-SBC-REQ from the MS/AMS selects the ASN-GW from the pool of available ASN-GWs in the "ASN-GW cluster" and sends MS Pre-attachment Req message to this ASN-GW. If the BS/ABS is pre-configured with the Authorization Policy in advance it may send an "early" SBC-RSP/AAI-SBC-RSP message to the MS/AMS in order to neutralize SBC-REQ retransmission timer (Wait for SBC-RSP timeout or Wait for AAI-SBC-RSP timeout).

4. If the ASN-GW accepts MS/AMS INE it shall respond back positively. If the ASN-GW rejects MS/AMS INE (e.g. because of overload) it may either (a) respond negatively sending MS Pre-Attachment Rsp message with Failure Indication TLV (5.3.2.69) set to indicate "no resources" or (b) respond positively sending MS Pre-Attachment Rsp message with Authenticator ID TLV (5.3.2.19) containing the redirected ASN-GW that has resources to support the INE request by the BS/ABS. In Figure 4-56, ASN-GW 1 responds negatively rejecting MS Pre-attachment transaction.

5. The BS/ABS confirms transaction completion by sending MS Pre-attachment Ack message to ASN-GW 1.

5a. If the ASN-GW 1 in step (4) sent positive MS Pre-attachment Rsp message with the Authenticator ID TLV (scenario (b)), the ASN-GW 1 triggers the "redirected" ASN-GW (ASN-GW 2) to initiate EAP authentication procedure. Messaging between ASN-GW 1 and the "redirected" ASN-GW 2 are out of the specification scope. Note, that step (5a) may occur in parallel to steps (3) – (5). Steps (6) – (8) are skipped in this case. Figure 4-57 shows the re-direction scenario.

6. If the ASN-GW 1 sent the failure indication TLV (scenario (a)), the BS/ABS selects the next available ASN-GW from the "ASN-GW cluster" and sends MS Pre-attachment Req message to this ASN-GW (ASN-GW 2 in the example shown in Figure 4-56). Note, that if the ASN-GW1 sent positive MS Pre-attachment Rsp message with the Authenticator ID TLV (scenario (b)), steps (6) – (8) are skipped (as shown in Figure 4-57) and the BS/ABS enters the Authentication Relay State (relaying R6 Auth Relay messages) and waiting for authentication completion (waiting for either Key Change Directive message or MS Network Exit signal).

7. ASN-GW 2 responds positively with MS Pre-attachment Rsp message.

8. BS/ABS confirms transaction completion by sending MS Pre-attachment Ack message to ASN-GW 2. By this ASN-GW selection process is complete.

9. ASN-GW 2 starts EAP transaction by sending Authentication Relay EAP-Transfer message to the BS/ABS with EAP-Request/ Identity payload.

10. The BS/ABS "relays" EAP message to the MS/AMS using PKMv2 EAP-Transfer or PKMv3 EAP-Transfer message.

11. Initial Network Entry process continues with the selected ASN-GW 2 acting as Authenticator and Anchor GW of the specific MS/AMS.

4.5.1.3.2 Case b - ASN-GW Redirection

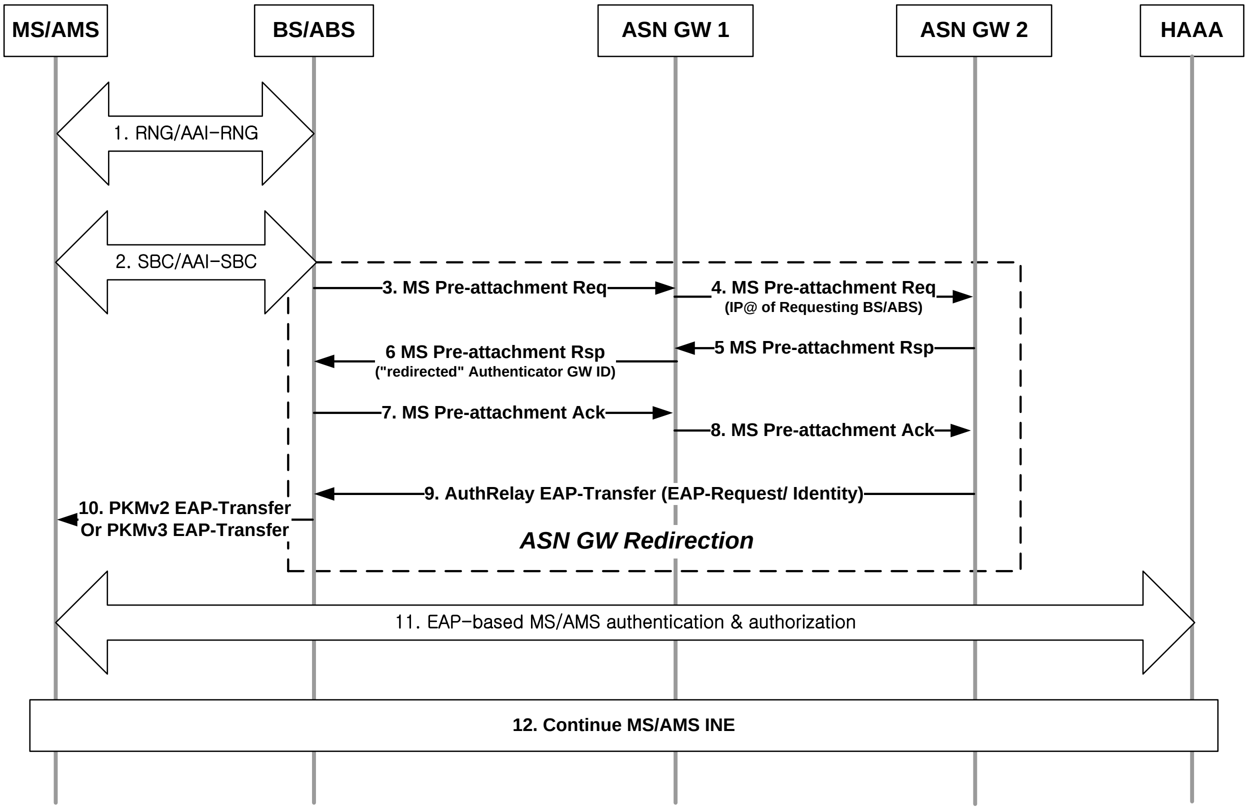


Figure 4-57 – ASN-GW re-direction during MS/AMS INE

1. The MS/AMS starts the INE process with the BS/ABS and performs a MAC Ranging.
2. After RNG/AAI-RNG exchange is completed, the MS/AMS performs SBC/AAI-SBC transaction with the BS/ABS.
3. The BS/ABS receiving SBC-REQ/AAI-SBC-REQ from the MS/AMS selects the ASN-GW from the pool of available ASN-GWs within the "ASN-GW cluster" and sends MS Pre-attachment Req message to the selected ASN-GW. The BS/ABS may send "early" SBC-RSP/AAI-SBC-RSP message to the MS/AMS in order to neutralize the SBC-REQ retransmission timer (Wait for SBC-RSP timeout or Wait for AAI-SBC-RSP timeout).
4. If the ASN-GW 1 can not accept the MS/AMS it sends MS-Pre-attachment Req (including IP Address of the Requesting BS TLV) to ASN-GW 2 (see Table 4-44).
5. ASN-GW 2 accepts the MS/AMS INE and therefore replies to ASN-GW with MS Pre-attachment Rsp.
6. ASN-GW 1 sends MS Pre-attachment Rsp (including Authenticator ID TLV with its value set to IP@ of ASN-GW 2) to the BS/ABS.
7. BS/ABS registers the value of Authenticator ID TLV from MS Pre-Attachment Rsp and sends MS-Pre-Attachment Ack to ASN-GW 1.
8. ASN-GW 1 sends MS Pre-Attachment Ack to ASN-GW 2.
9. ASN-GW 2 starts EAP transaction by sending Authentication Relay EAP-Transfer message to the BS/ABS with EAP-Request/ Identity payload.

10. The BS/ABS “relays” the EAP message to the MS/AMS using PKMv2 EAP-Transfer or PKMv3 EAP-Transfer message.

11. Initial Network Entry process continues with the selected ASN-GW 2 acting as Authenticator and Anchor GW of the specific MS/AMS.

4.5.1.4 Network Rejection Procedure

Figure 4-58 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/AMS is being denied access through this Network, such that the MS/AMS can act in a suitable manner.

When the Network Rejection is triggered, the EAP Notification Request is transmitted to the MS/AMS 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 [57]. After disconnection caused by the Network Rejection Procedure, the MS/AMS 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/AMS. 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/AMS side, the MS/AMS 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/AMS SHALL ignore the received Network Rejection Information.

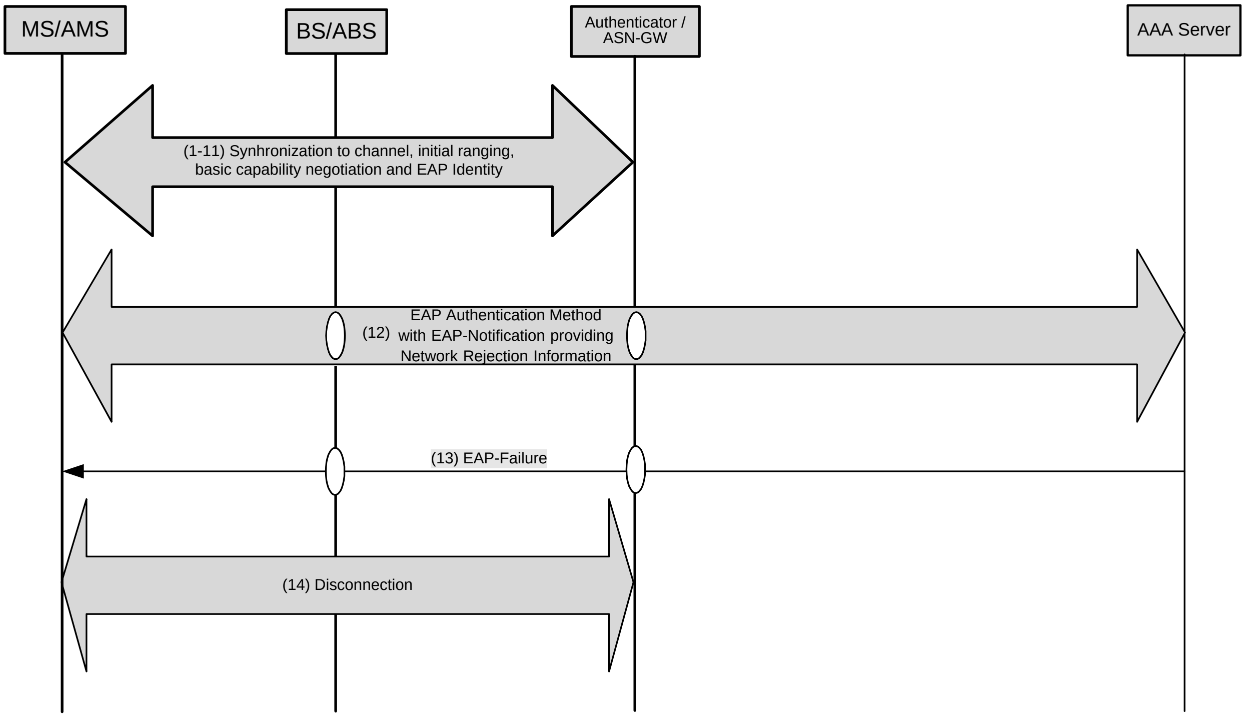

MS/AMS
BS/ABS
Authenticator / ASN-GW
AAA Server
(1-11) Synhronization to channel, initial ranging, basic capability negotiation and EAP Identity
(12)
EAP Authentication Method with EAP-Notification providing Network Rejection Information
(13) EAP-Failure
(14) Disconnection

Figure 4-58 – 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/ABS 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/AMS and AAA server.

When the Visited NSP decides to initiate the Network Rejection with the MS/AMS 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/AMS by not forwarding any AAA messages towards the Home NSP. Furthermore, the VAAA SHALL negotiate the use of EAP-TLS with the MS/AMS.

The local AAA server includes its own certificate with the EAP-TLS server_hello message. When the MS/AMS receives a AAA server certificate, the MS/AMS SHALL validate the AAA server certificate and act as defined in the section 4.4.1.2. If MS/AMS receives network rejection information from a VNSP, different than the one chosen during ND&S, the MS/AMS 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/AMS 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 4-59 ~ Figure 4-62 illustrate possible Network Rejection flow examples for the EAP-TLS, EAP-TTLS, and EAP-AKA, respectively.

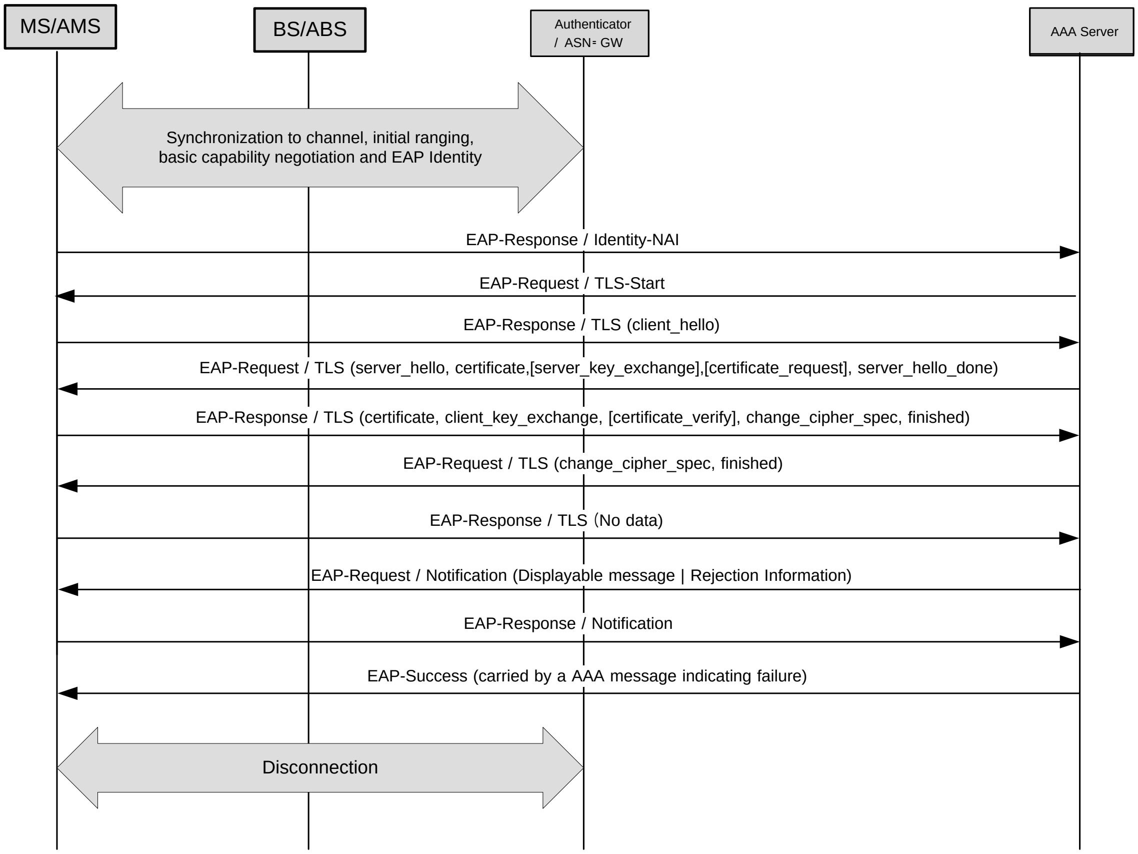

MS/AMS
BS/ABS
Authenticator / ASN- GW
AAA Server
Synchronization to channel, initial ranging, basic capability negotiation and EAP Identity
EAP-Response / Identity-NAI
EAP-Request / TLS-Start
EAP-Response / TLS (client_hello)
EAP-Request / TLS (server_hello, certificate,[server_key_exchange],[certificate_request], server_hello_done)
EAP-Response / TLS (certificate, client_key_exchange, [certificate_verify], change_cipher_spec, finished)
EAP-Request / TLS (change_cipher_spec, finished)
EAP-Response / TLS (No data)
EAP-Request / Notification (Displayable message | Rejection Information)
EAP-Response / Notification
EAP-Success (carried by a AAA message indicating failure)
Disconnection

Figure 4-59 – Network Rejection Procedure for EAP-TLS

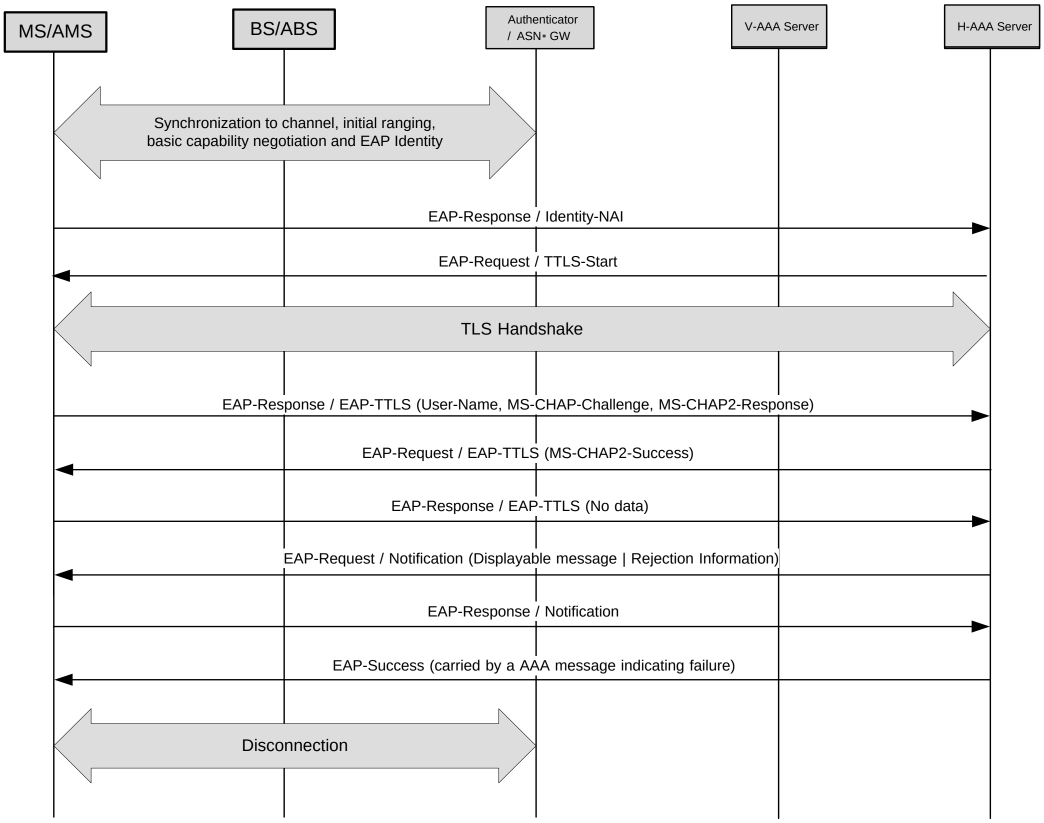

MS/AMS
BS/ABS
Authenticator / ASN- GW
V-AAA Server
H-AAA Server
Synchronization to channel, initial ranging, basic capability negotiation and EAP Identity
EAP-Response / Identity-NAI
EAP-Request / TTLS-Start
TLS Handshake
EAP-Response / EAP-TTLS (User-Name, MS-CHAP-Challenge, MS-CHAP2-Response)
EAP-Request / EAP-TTLS (MS-CHAP2-Success)
EAP-Response / EAP-TTLS (No data)
EAP-Request / Notification (Displayable message | Rejection Information)
EAP-Response / Notification
EAP-Success (carried by a AAA message indicating failure)
Disconnection

Figure 4-60 – Network Rejection Procedure for EAP-TTLS

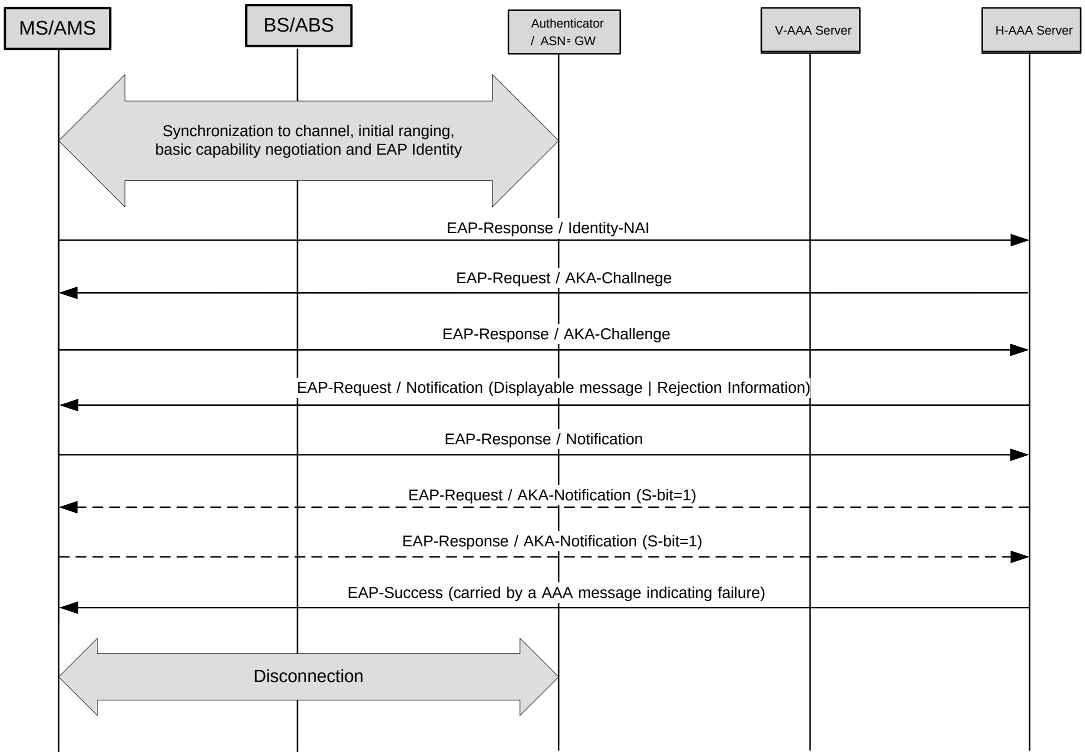

MS/AMS
BS/ABS
Authenticator / ASN¤ GW
V-AAA Server
H-AAA Server
Synchronization to channel, initial ranging, basic capability negotiation and EAP Identity
EAP-Response / Identity-NAI
EAP-Request / AKA-Challnege
EAP-Response / AKA-Challenge
EAP-Request / Notification (Displayable message | Rejection Information)
EAP-Response / Notification
EAP-Request / AKA-Notification (S-bit=1)
EAP-Response / AKA-Notification (S-bit=1)
EAP-Success (carried by a AAA message indicating failure)
Disconnection

Figure 4-61 – 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 4-62shows an example of the Network Rejection with the EAP-Failure.

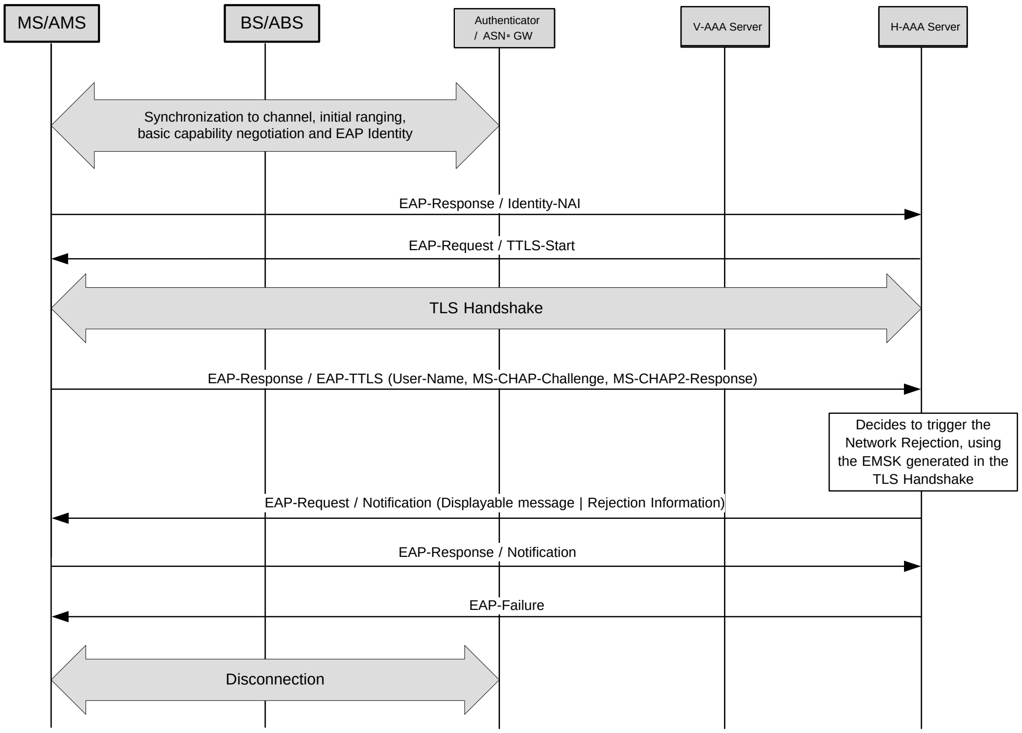

MS/AMS
BS/ABS
Authenticator / ASN- GW
V-AAA Server
H-AAA Server
Synchronization to channel, initial ranging, basic capability negotiation and EAP Identity
EAP-Response / Identity-NAI
EAP-Request / TTLS-Start
TLS Handshake
EAP-Response / EAP-TTLS (User-Name, MS-CHAP-Challenge, MS-CHAP2-Response)
Decides to trigger the Network Rejection, using the EMSK generated in the TLS Handshake
EAP-Request / Notification (Displayable message | Rejection Information)
EAP-Response / Notification
EAP-Failure
Disconnection

Figure 4-62 – Network Rejection Procedure in case of EAP-TTLS phase 2 Failure

Figure 4-62 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/AMS 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/AMS determines the network access authorization result from the received EAP-Notification, and ASN makes the same determination from the received AAA message.

STEP 14

Authenticator proceeds with disconnection procedure following Access-Reject/Diameter WDEA as defined in [1].

4.5.1.4.1 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/AMS 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 BS/ABSs. A Rejection Class is a group of Rejection Codes that have a common MS/AMS handling in terms of Security Category, Rejection duration/criteria, Applicability for Visited/Home AAA and scope of rejection.

The MS/AMS 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/AMS by adding an Emergency Services Override TLV to the Network Rejection Information.

When an MS/AMS is rejected from all the NSPs connected through an NAP, the MS/AMS may continue to verify which NSP are available through other BS/ABSs advertising the same NAP ID.

4.5.1.4.2 Rejection Classes

The following provides information on the handling required at the MS/AMS 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/AMS is again allowed to access the network.

If the MS/AMS receives the Rejection Duration/Criteria indicating “Until Manual Retry”, the MS/AMS 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/AMS 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/AMS receives the Rejection Duration/Criteria indicating “Until Power Cycle”, the MS/AMS SHALL NOT access a network with the “Scope of Rejection” until the MS/AMS 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/AMS receives the Rejection Duration/Criteria indicating “Until Timer Expiry”, the MS/AMS 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/AMS SHALL double the Network Rejection Timer. The maximum value of the Network Rejection Timer SHALL be 6 hours. When the MS/AMS successfully registers through an NSP with the “Scope of Rejection” the MS/AMS SHALL reset the start value of the Network Rejection Timer.

If the MS/AMS receives the Rejection Duration/Criteria indicating “Until Device is upgraded or until CVS Timer Expiry”, the MS/AMS 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/AMS SHALL double the CVS Network Rejection Timer. The maximum value of the CVS Network Rejection Timer SHALL be 4 weeks. When the MS/AMS successfully registers through an NSP with the “Scope of Rejection” the MS/AMS SHALL reset the start value of the Network Rejection Timer.

If the MS/AMS receives the Rejection Duration/Criteria indicating “Until Location Criteria met”, the MS/AMS SHALL NOT access a network with the “Scope of Rejection” until the MS/AMS has moved to a BS/ABS 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/AMS SHALL only treat the current BS/ABS 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/AMS receives a Rejection code from a Rejection Class from the Visited AAA where the Applicability is limited to the Home AAA, the MS/AMS SHALL ignore the Network Rejection Information. That means, the Visited AAA can reject the MS/AMS 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/AMS has been rejected from each of the NSPs connected to a NAP, the MS/AMS 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/AMS 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/AMS is de-registered from network service and its context is deleted.

The following entities may start MS De-registration process:

- MS/AMS, 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 De-registration.

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/ABS (and probably re-initialization in other (A)BS/Network);
- Enforcing MS/AMS to halt any transmissions (including MAC management messaging);
- Enforcing MS/AMS to halt traffic transmissions;
- Erasing MS context in the ASN entities when radio link with the MS/AMS has been lost.

De-registration signaling over R1 Reference Point (over the air) is done using IEEE 802.16 defined messages with the specific Action/ De-registration_Request_Code parameters:

- DREG-CMD/AAI-DREG-RSP – message used by BS/ABS to signal de-registration command to MS/AMS. It may be unsolicited or in response to MS-initiated DREG-REQ/AMS-initiated AAI-DREG-REQ. DREG-CMD/AAI-DREG-RSP message should include Action Code parameter indicating the requested de-registration action;
- DREG-REQ/AAI-DREG-REQ – MS/AMS sends this message to BS/ABS to request de-registration. This message should include De-registration_Request_Code parameter indicating the reason of de-registration request.

4.5.2.1 Normal Mode

In the normal mode, considering MS/AMS 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/AMS Triggered Network Exit

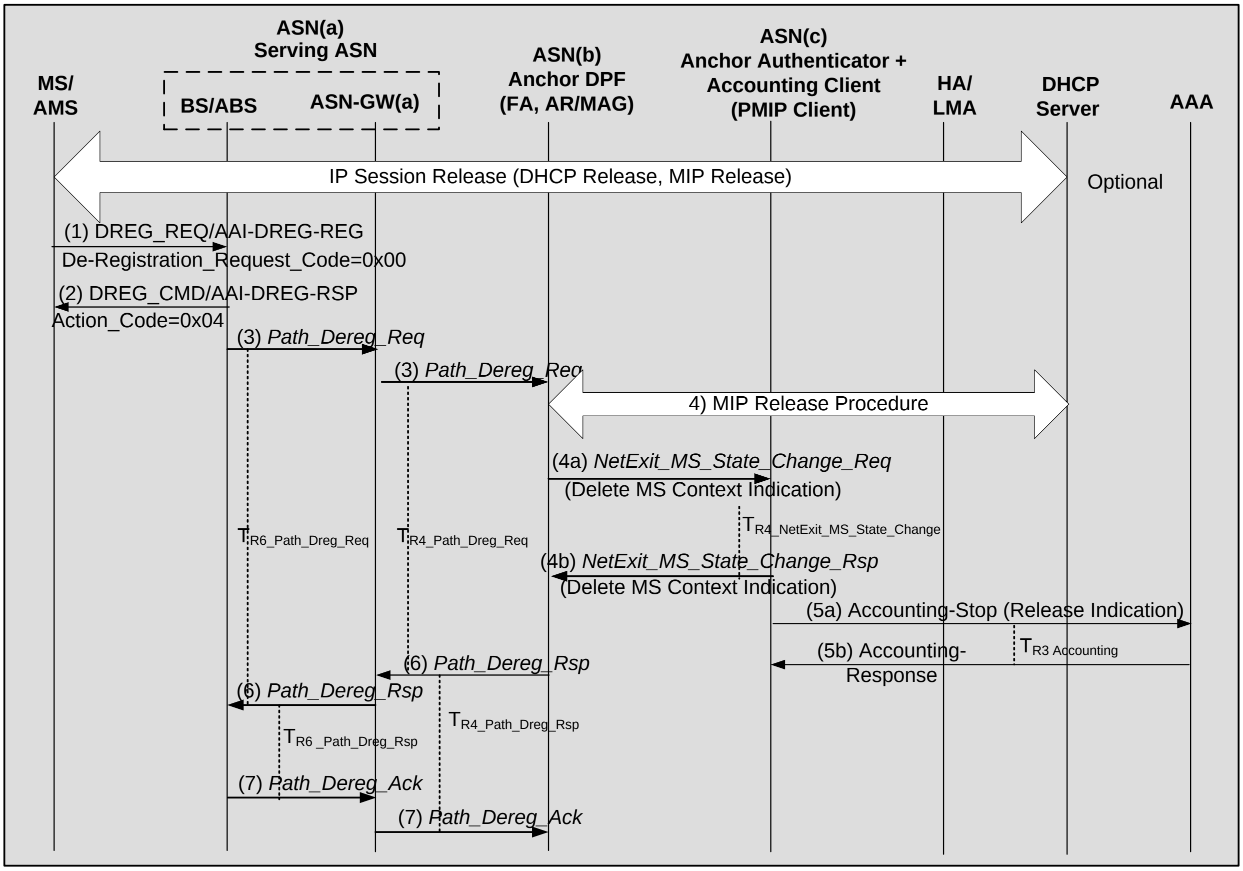


Figure 4-63 – MS/AMS Triggered Network Exit (Normal Mode)

STEP 1

While the MS/AMS has an active session the MS/AMS exits the network by sending a DREG-REQ/AAI-DREG-REQ message to BS/ABS in Serving ASN, including De-Registration_Request Code=0x00.

Before this step, optionally, MS/AMS performs initiating DHCP Release Procedure and for a CMIP terminal, MS/AMS 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/ABS sends DREG-CMD/AAI-DREG-RSP message to the MS/AMS including Action Code=0x04.

STEP 3

BS/ABS 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 step 1, the ASN(b) can perform a MIP De-Registration as specified in 4.8.3.4.

For PMIP4, if MS/AMS 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 4.8.2.4.8.

For PMIP6, if there was no DHCPv4/v6 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 turn sends a *Path_Dereg_Rsp* message over R6 to the BS.

STEP 7

The BS/ABS 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 data path resource for the MS/AMS.

4.5.2.1.2 Network Trigger

The following network entities may initiate MS Network Exit:

- Home AAA server;
- Authenticator/PMIP client;
- Anchor DPF/FA or MAG, DHCP proxy/relay;
- Serving (A)BS/Serving ASN;
- HA, LMA.

Network Exit may be initiated in situations where Data Path for the MS/AMS has already been established or not. Regardless of the data path existence, either Data Path Control (*Path_Dereg_Reg/Rsp*) or *NetExit_MS_State_Change_Req*/*Rsp* messages may be used (means a BS/ABS 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 DPF and Authenticator), *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/ABS to perform MS de-registration may involve Data Path Control messages (*Path_Dereg_Req/Rsp*) between Anchor DPF and BS/ABS 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/ABS).

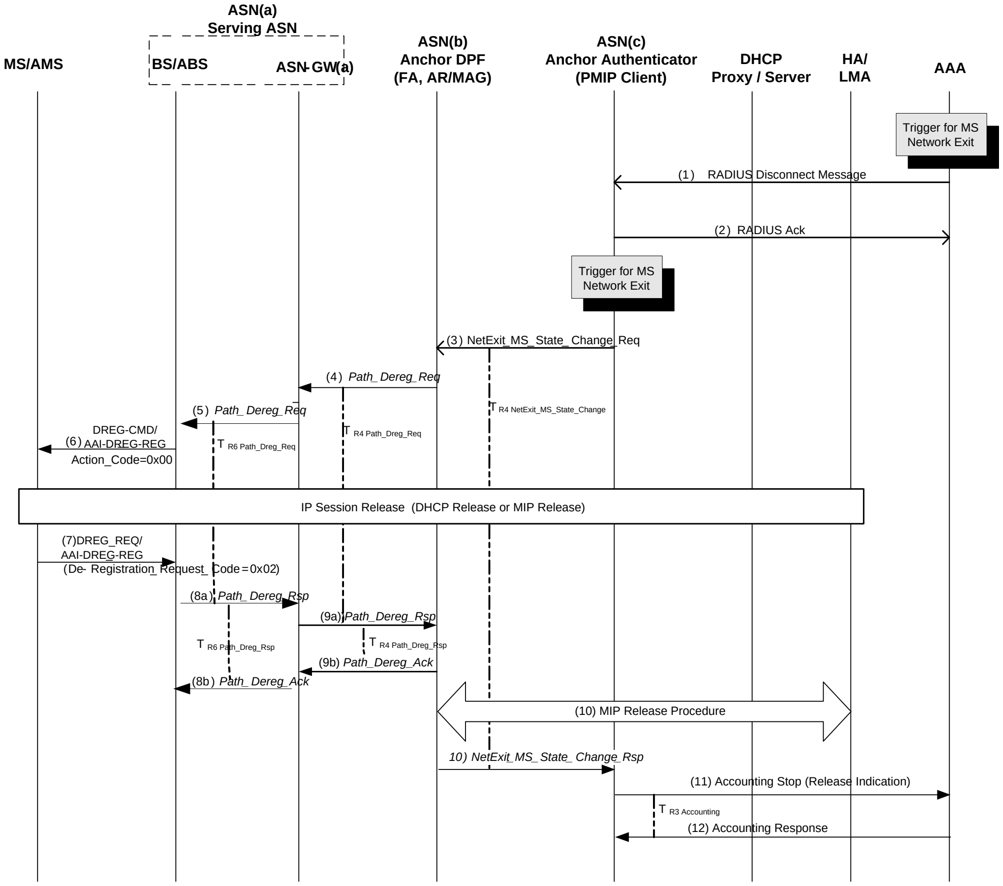


Figure 4-64 – AAA Server/Authenticator Trigger (Normal Mode)

STEP 1

Home-AAA server in the Home CSN takes a decision to de-register the MS/AMS based on changing service strategy including user's arrearage, report loss of mobile phone by user, etc.

The H-AAA sends RADIUS Disconnect-Request 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-Request 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 5.5.1.1.6 for Diameter. If NAS cannot proceed with MS de-registration, it should respond with RADIUS Disconnect-NACK message or Diameter WASA command indicating failure as presented in 5.4.1.6.9 and 5.5.1.1.6.

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 de-registration process by sending a *NetExit_MS_State_Change_Req* message over R4 to ASN(b) including Action Code TLV set to indicate MS De-registration from the network.

For PMIP4, 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.

For PMIP6, MS/AMS may perform DHCPv4/v6 release procedure triggering ASN(b) to initiate PMIP6 release procedure. If MS/AMS did not perform DHCPv4/v6 Release or if MIP De-Registration was not triggered prior, the ASN(b) SHALL perform PMIP6 session release procedure with the LMA as described in Section 4.8.5.6.

If the authenticator located in ASN(a), the authenticator can initiate by sending a *NetExit_MS_State_Change_Req* message to a BS/ABS directly including Action Code TLV set to indicate MS De-registration 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 de-registration procedure toward the Serving BS/ABS by sending *Path_Dereg_Req* message over R4 to the Serving ASN(a) with Action Code TLV set to indicate MS De-registration from the network.

STEP 5

The Serving ASN(a) forwards *Path_Dereg_Req* message over R6 with Action Code TLV to the Serving BS/ABs.

STEP 6

BS/ABS initiates over-the-air MS de-registration process according to the value specified in the Action Code TLV (e.g., by sending DREG-CMD/AAI-DREG-RSP message to MS/AMS 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/ABS should use the corresponding operation over-the-air DREG-CMD/AAI-DREG-RSP with appropriate Action Code or RES-CMD/AAI-RES-CMD.

STEP 7

MS/AMS replies with DREG-REQ/AAI-DREG-REQ message to BS/ABS including De-registration_Request_Code = 0x02.

Before this step, for CMIP terminal, MS/AMS may perform MIP release procedure. For PMIP4, MS/AMS may perform DHCP release procedure. This DHCP Release triggers PMIP4 client to initiate MIP release procedure. For PMIP6, the MS/AMS may perform DHCPv4/v6 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/ABS does not receive DREG-REQ/AAI-DREG-REQ message from MS/AMS, it should be able to detect the completion of over-the-air MS de-registration procedure and then follow the next steps.

STEP 8

BS/ABS responds to *Path_Dereg_Req* message from Serving ASN(a) by *Path_Dereg_Rsp* message. This step occurs when BS/ABS detects the completion of over-the-air MS de-registration procedure.

Serving ASN(a) acknowledges the receipt of *Path_Dereg_Rsp* message by sending *Path_Dereg_Ack* message over R6 to the BS/ABS.

STEP 9

The Serving ASN(a) proceeds with data path de-registration 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 de-registration 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 PMIP4, if MS/AMS did not perform DHCP Release procedure in the step 7, the ASN(c) SHALL perform MIP De-Registration.

For PMIP6, if MS/AMS did not perform DHCPv4/v6 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

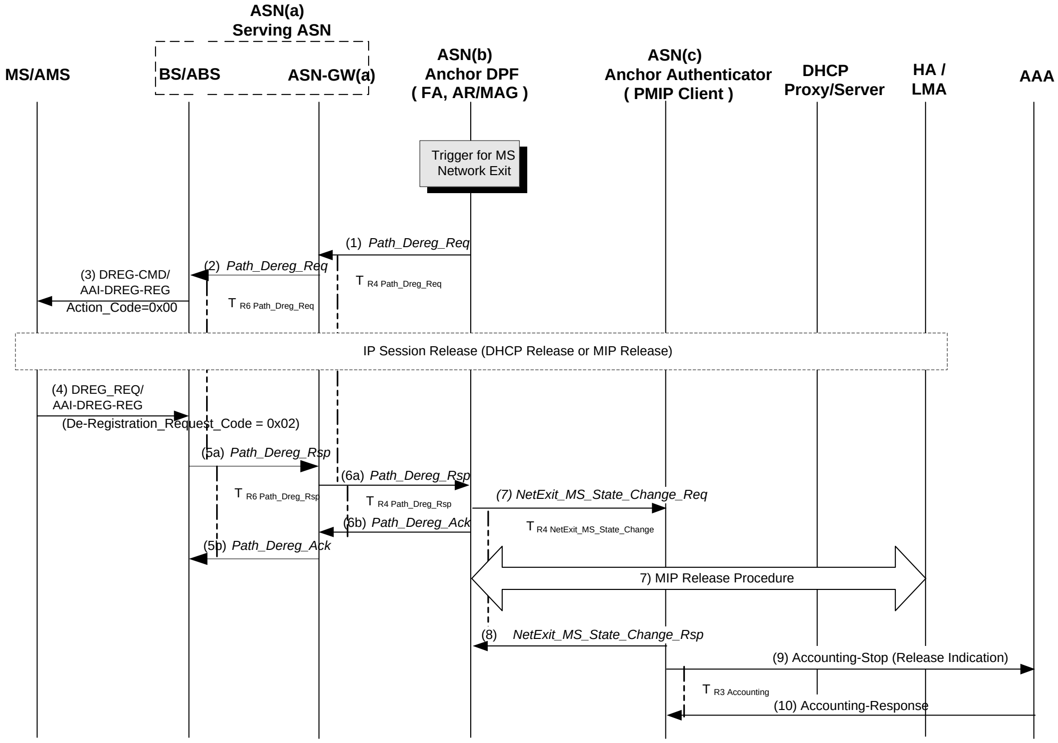


Figure 4-65 – Anchor DPF/FA Triggered Network Exit (Normal Mode)

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 de-registration procedure along the data path by sending *Path_Dereg_Req* message over R4 with Action Code TLV set to indicate MS De-registration 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 de-registration 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 PMIP4, 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/ABS - initiated MS Network Exit

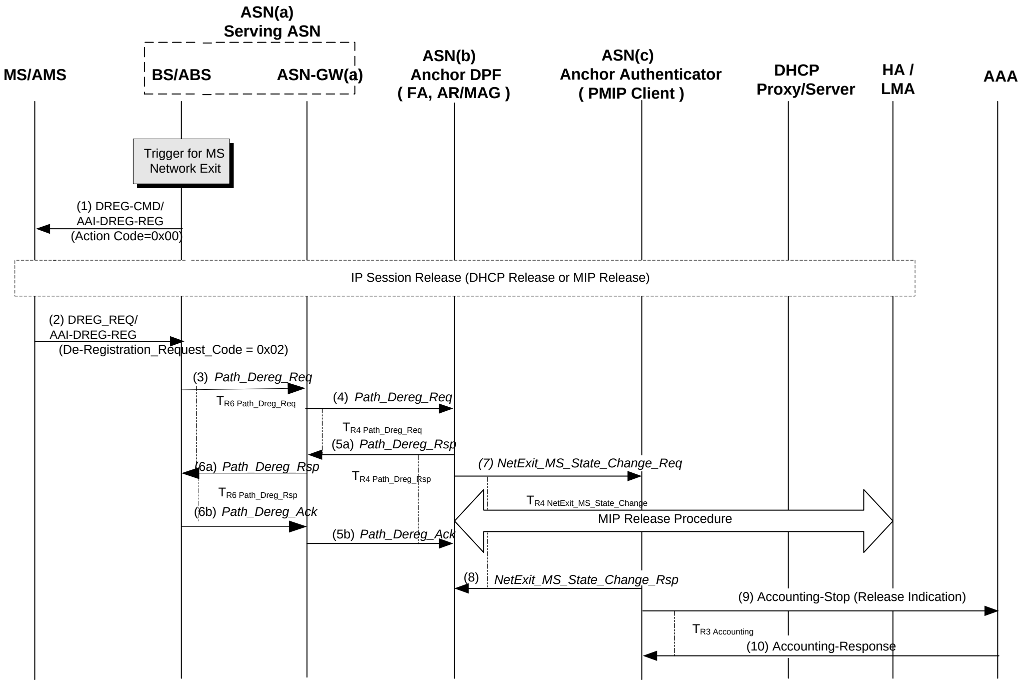

ASN(a)
Serving ASN
MS/AMS
BS/ABS
ASN-GW(a)
ASN(b)
Anchor DPF
(FA, AR/MAG)
ASN(c)
Anchor Authenticator
(PMIP Client)
DHCP
Proxy/Server
HA /
LMA
AAA
Trigger for MS Network Exit
(1) DREG-CMD/ AAI-DREG-REG (Action Code=0x00)
IP Session Release (DHCP Release or MIP Release)
(2) DREG_REQ/ AAI-DREG-REG (De-Registration_Request_Code = 0x02)
(3) Path_Dereg_Req
$T_{R6\ Path\_Dreg\_Req}$
(4) Path_Dereg_Req
$T_{R4\ Path\_Dreg\_Req}$
(5a) Path_Dereg_Rsp
(6a) Path_Dereg_Rsp
$T_{R4\ Path\_Dreg\_Rsp}$
(7) NetExit_MS_State_Change_Req
$T_{R6\ Path\_Dreg\_Rsp}$
$T_{R4\ NetExit\_MS\_State\_Change}$
MIP Release Procedure
(6b) Path_Dereg_Ack
(5b) Path_Dereg_Ack
(8) NetExit_MS_State_Change_Rsp
(9) Accounting-Stop (Release Indication)
$T_{R3\ Accounting}$
(10) Accounting-Response

Figure 4-66 – BS/ABS Triggered Network Exit (Normal Mode)

STEP 1

MS Network Exit trigger occurs in the Serving BS/ABS. Generally, BS/ABS in the Serving ASN should not be an initiator of MS De-registration. 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/ABS may start MS De-registration process by sending the DREG-CMD/AAI-DREG-RSP to the MS/AMS.

BS/ABS sends DREG-CMD/AAI-DREG-RSP message to MS/AMS including Action Code =0x00 to enforce MS network exit.

STEP 2

MS/AMS replies with DREG-REQ/AAI-DREG-REQ message to BS/ABS including De-registration_Request_Code = 0x02.

Before this step, for CMIP terminal, MS/AMS may perform MIP release procedure. For PMIP4, MS/AMS may perform DHCP release procedure. This DHCP Release triggers PMIP4 client to initiate MIP release procedure. For PMIP6, MS/AMS may perform DHCPv4/v6 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/ABS does not receive DREG-REQ/AAI-DREG-REQ message from MS/AMS, it should be able to detect the completion of over-the-air MS de-registration procedure and then follow the next steps.

STEP 3

BS/ABS sends *Path_Dereg_Req* message with Network Exit Indicator along the data path to Serving ASN(a). This step occurs when BS/ABS detects the completion of over-the-air MS de-registration procedure.

STEP 4

The Serving ASN(a), receiving *Path_Dereg_Req* message with Network Exit Indicator, proceeds with data path de-registration 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/ABS over R6.

BS/ABS, 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/ABS

As mentioned above, Network Exit initiated by ASN entities may be using *NetExit_MS_State_Change_Req*/*Rsp* messages to instigate Network Exit procedure from a BS/ABS. The example of such flow initiated by ASN GW (a) is presented in this subsection.

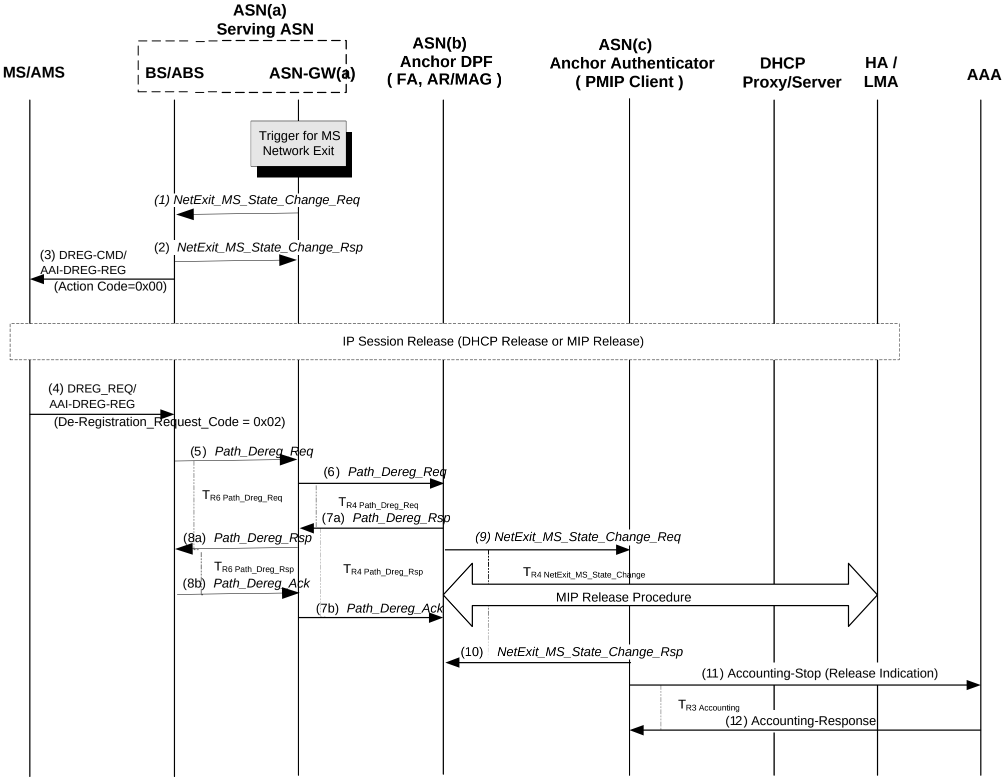


Figure 4-67 – ASN entity instigating Network Exit in a BS/ABS

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/ABS with Action Code TLV set to indicate MS De-registration from the network.

STEP 2

BS/ABS in ASN(a) responds by sending *NetExit_MS_State_Change_Rsp* message over R6 to the ASN-GW(a).

STEP 3

BS/ABS in ASN(a) initiates over-the-air MS de-registration process according to the value specified in the Action Code TLV (e.g., by sending DREG-CMD/AAI-DREG-RSP message to MS/AMS 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/ABS should use the corresponding operation over-the-air DREG-CMD/AAI-DREG-RSP with appropriate Action Code, RES-CMD/AAI-RES-CMD or RNG-RSP/AAI-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

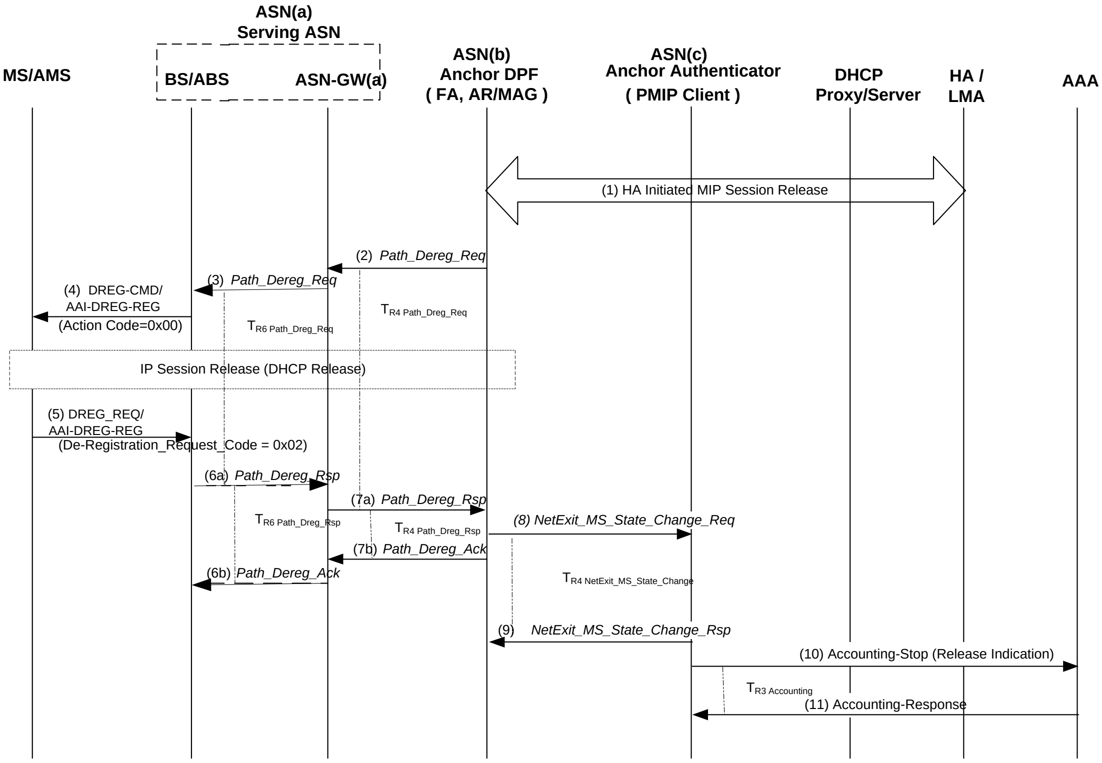


Figure 4-68 – HA/LMA Triggered MS Network Exit

STEP 1

HA decides to De-register the MS/AMS from the network and performs PMIP Session release for the MS/AMS as specified in section 4.8.2.4.8.1.3. For CMIP case the MIP de-registration is performed between the MS/AMS, 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/AMS unknown about the MIP De-registration for, PMIP case, may optionally send DHCP_RELEASE. 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/AMS Triggered Network Exit (Idle Mode)

There are two options for an MS/AMS to trigger network exit while it is in idle mode:

- MS/AMS 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/AMS sends RNG-REQ/AAI-RNG-REQ with power down indication without exiting the idle mode. The following call procedure is for this network exit method.

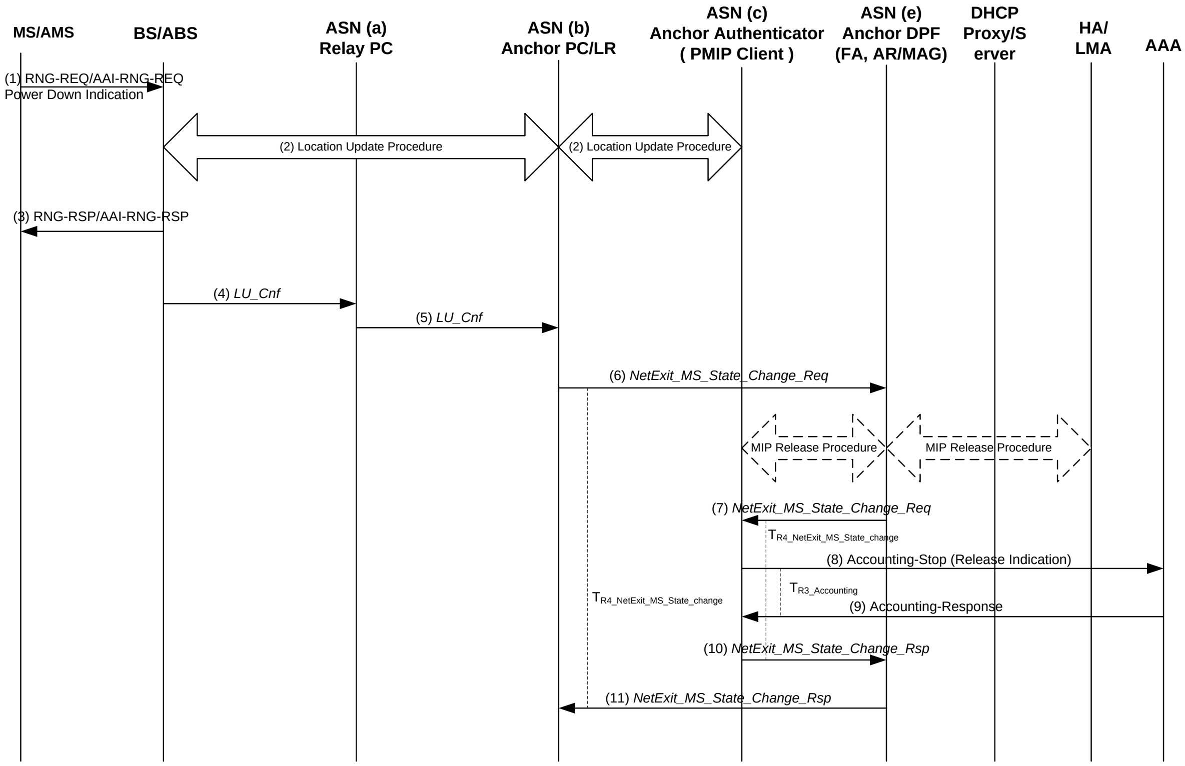

MS/AMS
BS/ABS
ASN (a) Relay PC
ASN (b) Anchor PC/LR
ASN (c) Anchor Authenticator (PMIP Client)
ASN (e) Anchor DPF (FA, AR/MAG)
DHCP Proxy/S erver
HA/ LMA
AAA
(1) RNG-REQ/AAI-RNG-REQ Power Down Indication
(2) Location Update Procedure
(2) Location Update Procedure
(3) RNG-RSP/AAI-RNG-RSP
(4) LU_Cnf
(5) LU_Cnf
(6) NetExit_MS_State_Change_Req
MIP Release Procedure
MIP Release Procedure
(7) NetExit_MS_State_Change_Req
TR4_NetExit_MS_State_change
(8) Accounting-Stop (Release Indication)
TR3_Accounting
TR4_NetExit_MS_State_change
(9) Accounting-Response
(10) NetExit_MS_State_Change_Rsp
(11) NetExit_MS_State_Change_Rsp

Figure 4-69 – MS Triggered Network Exit (Idle Mode)

STEP 1

During the Idle Mode, MS/AMS decide to power down, MS/AMS sends RNG-REQ/AAI-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/ABS verifies successfully the RNG-REQ/AAI-RNG-REQ message based on MS/AMS's AK and AK Context, (A)BS/PA and ASN(b) together with Anchor PC SHALL perform a normal location update procedure.

STEP 3, 4, 5

The BS/ABS replies with RNG-RSP/AAI-RNG-RSP to the MS/AMS 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/AMS 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(d)/Anchor DPF/FA.

STEP 7, 10

ASN(d)/Anchor DPF sends *NetExit_MS_State_Change_Req* over R4 including Delete MS Context Indication to ASN(c)/Anchor Authenticator.

For CMIP4, PMIP4, and PMIP6 session, before this step, ASN(d)/Anchor DPF SHALL initiate the MIP De-Registration procedure. For CMIP, the FA can perform MIP Revocation procedure based on [51]. Additionally the associated entities SHALL release the related MS context and resource retained by these entities. For PMIP4, ASN(c) containing the Anchor PMIP4 client, ASN(d) containing the FA and the HA can complete a MIP De-Registration procedure based on the normal MIP De-registration procedure. For PMIP6, the AR/MAG can perform MIP Revocation procedure based on [96]. 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/AMS 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(d)/Anchor DPF sends over R4 a *NetExit_MS_State_Change_Rsp* 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/AMS and let the MS/AMS perform graceful Network Exit Procedure, Network MAY clean up the resources for the given MS/AMS. 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.

4.5.2.2.2.1.1 AAA Server or Authenticator - initiated Network Exit in Idle Mode

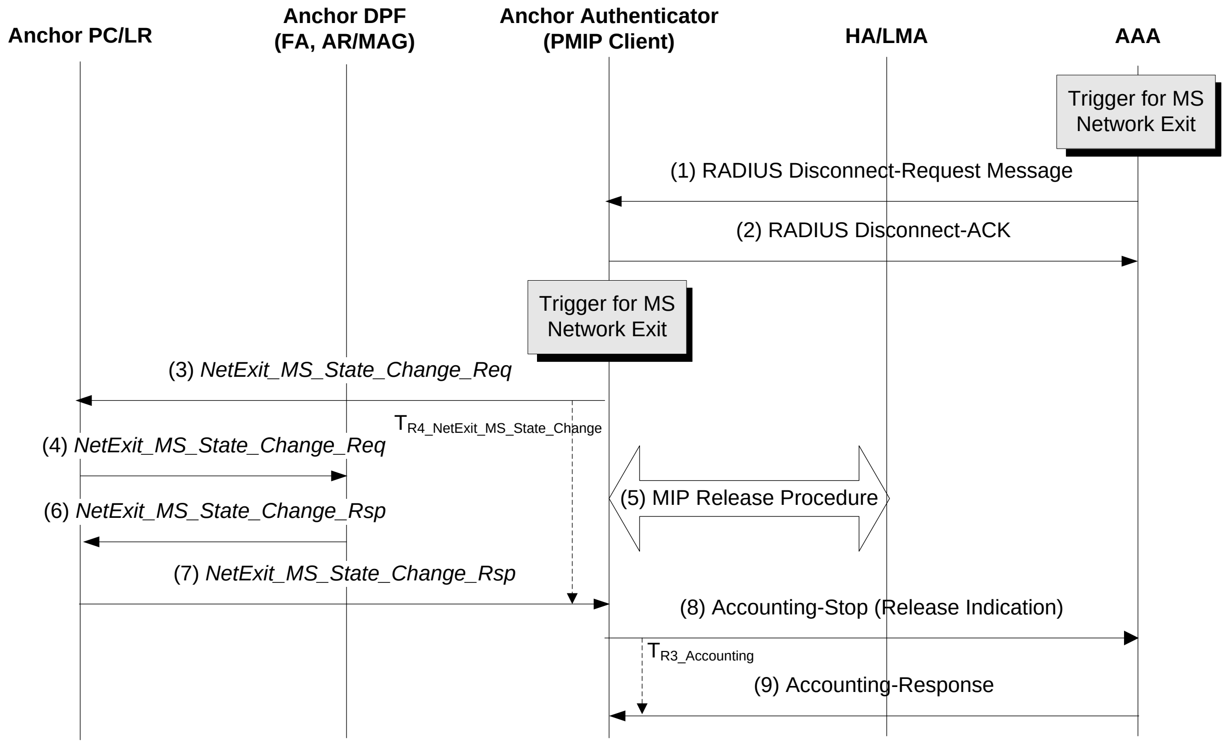

Anchor PC/LR
Anchor DPF (FA, AR/MAG)
Anchor Authenticator (PMIP Client)
HA/LMA
AAA
Trigger for MS Network Exit
(1) RADIUS Disconnect-Request Message
(2) RADIUS Disconnect-ACK
Trigger for MS Network Exit
(3) NetExit_MS_State_Change_Req
TR4_NetExit_MS_State_Change
(4) NetExit_MS_State_Change_Req
(5) MIP Release Procedure
(6) NetExit_MS_State_Change_Rsp
(7) NetExit_MS_State_Change_Rsp
(8) Accounting-Stop (Release Indication)
TR3_Accounting
(9) Accounting-Response

Figure 4-70 – AAA Server/Authenticator Triggered Ungraceful Network Exit (Idle Mode)

STEP 1

When AAA server decides to disconnect the MS/AMS, the AAA MAY initiate the procedure by sending RADIUS Disconnect-Request Message or Diameter WASR command to Authenticator.

STEP 2

The Authenticator (NAS) acknowledges RADIUS Disconnect-Request 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/AMS related context.

STEP 5

The Authenticator triggers the Mobile IP Release procedure.

For PMIP4 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 releases the retained MS context.

STEP 7

The PC deletes all the MS/AMS 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).

4.5.2.2.2.1.2 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/AMS.

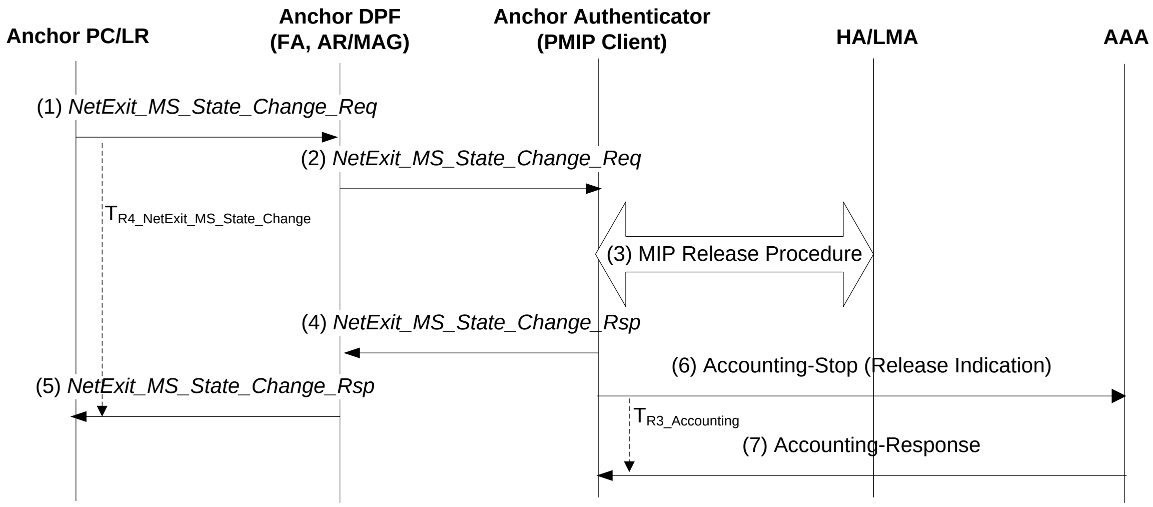

Anchor PC/LR
Anchor DPF (FA, AR/MAG)
Anchor Authenticator (PMIP Client)
HA/LMA
AAA
(1) NetExit_MS_State_Change_Req
(2) NetExit_MS_State_Change_Req
T_R4_NetExit_MS_State_Change
(3) MIP Release Procedure
(4) NetExit_MS_State_Change_Rsp
(6) Accounting-Stop (Release Indication)
(5) NetExit_MS_State_Change_Rsp
T_R3_Accounting
(7) Accounting-Response

Figure 4-71 – 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 PMIP4 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 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 releases 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.

4.5.2.2.2.1.3 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.

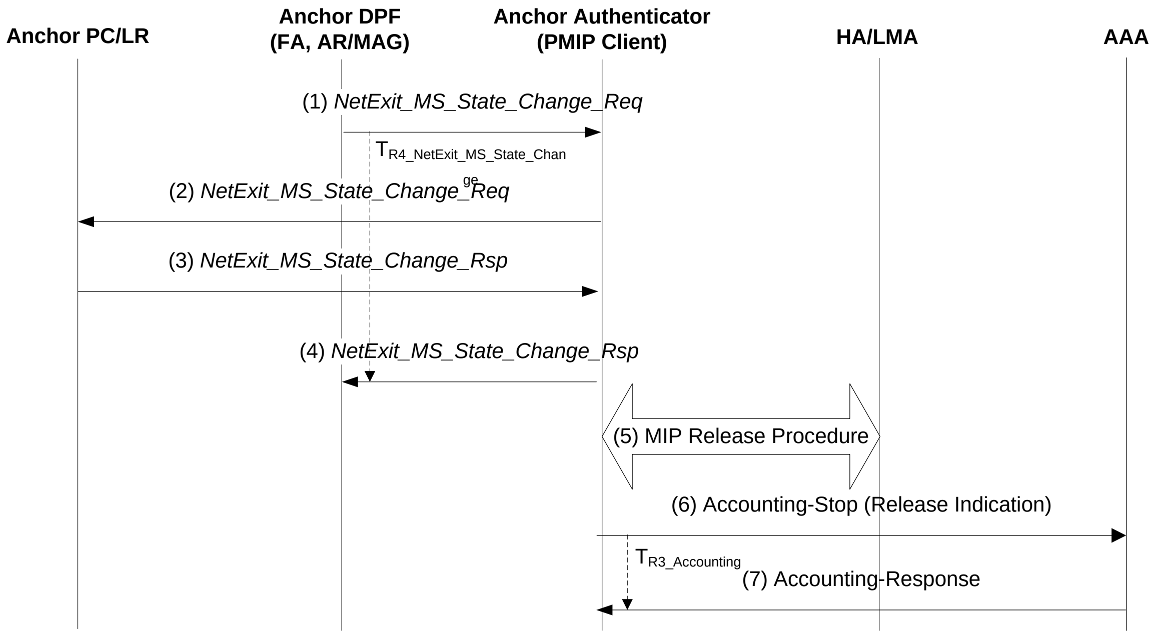

Anchor PC/LR
Anchor DPF
(FA, AR/MAG)
Anchor Authenticator
(PMIP Client)
HA/LMA
AAA
(1) NetExit_MS_State_Change_Req
T R4_NetExit_MS_State_Change
(2) NetExit_MS_State_Change_Req
(3) NetExit_MS_State_Change_Rsp
(4) NetExit_MS_State_Change_Rsp
(5) MIP Release Procedure
(6) Accounting-Stop (Release Indication)
T R3_Accounting
(7) Accounting-Response

Figure 4-72 – 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/AMS.

STEP 3

The PC deletes all the MS/AMS 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 PMIP4 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 4.5.2.2.2.1.2. 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 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 4-54:

Table 4-54 – 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/AMS at the time of initial network entry.
DCR Indication	5.3.2.530	O	Present if the message is generated as a result of an AMS entering DCR mode
BS Info	5.3.2.26	M	Compound TLV including information about BS/ABS.
>BS ID	5.3.2.25	M	Unique BS Identifier.
Action Code	5.3.2.3	O	De-registration instruction for the MS/AMS. Included only when the message is directed to a Serving BS/ABS 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/AMS is lost, etc.).
Ungraceful Network Exit Indicator	5.3.2.274	O[6]	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/AMS.
>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.

[6] "Ungraceful Network Exit Indication" TLV is presented for network triggered ungraceful network exit in idle mode.

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 4-55:

Table 4-55 – 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/AMS 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	

4.5.2.3.2 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 5.5.1.1.6:

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_Dereg_Req* and stopped upon the reception of the *Path_Dereg_Rsp.*

$T_{R4\_Path\_Dreg\_Req}$: This Timer is started by ASN-GW(a) upon transmission of *Path_Dereg_Req* to ASN(b) Anchor DPF and stopped upon the reception of the *Path_Dereg_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_Dereg_Rsp* and stopped upon reception of *Path_Dereg_Ack.*

$T_{R4\_Path\_Dreg\_Rsp}$: This Timer is started by ASN(b) Anchor DPF upon transmission of *Path_Dereg_Rsp* and stopped upon reception of *Path_Dereg_Ack .*

Table 4-56 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 1.6.

Table 4-56 – 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 4-57 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 4-57.

Table 4-57 – Actions after Timer Max Retry

Timer	Entity where Timer Started	Action(s)
$T_{R6\_Path\_Dreg\_Req}$	BS/ABS	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
$T_{R4\_Path\_Dereg\_Rsp}$	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 WiMAX Forum® Network Architecture 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:

a. Pre-provisioned Service Flow creation, modification, and deletion.

b. Initial Service Flow (ISF) creation, modification, and deletion.

c. Default Service Flow (DSF) creation, modification, and deletion

d. Dynamic Service Flow creation, modification, and deletion

e. Static QoS policy provisioning between AAA and Anchor-SFA.

f. Service Flow ID management.

g. Modification of existing ISF, DSF, 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/AMS, 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. WiMAX Forum® Network Architecture 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/AMS 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 4-81 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/AMS is set, the MS/AMS 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 (section5.4.1.1) 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/AMS, a separate pair of ISFs is required.

The purpose of the ISF is that it is used by the MS/AMS 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.

If any of the initial service flows of a given CS type for the associated MS/AMS is failed to be activated by the local ASN, the MS/AMS SHALL be denied of the service for the given CS type. If none of the CS types can be activated successfully for the MS/AMS, the MS/AMS SHALL be denied of the service by the local ASN. Otherwise, if at least one of the CS types of the MS/AMS is operational, the ASN SHALL continue the support the MS/AMS operation at the local ASN.

The number of retries for the local ASN to attempt to establish the ISFs for the given CS type is local network policy decision and is outside the scope of this specification.

4.6.4.2.1 IP-CS Related Issues

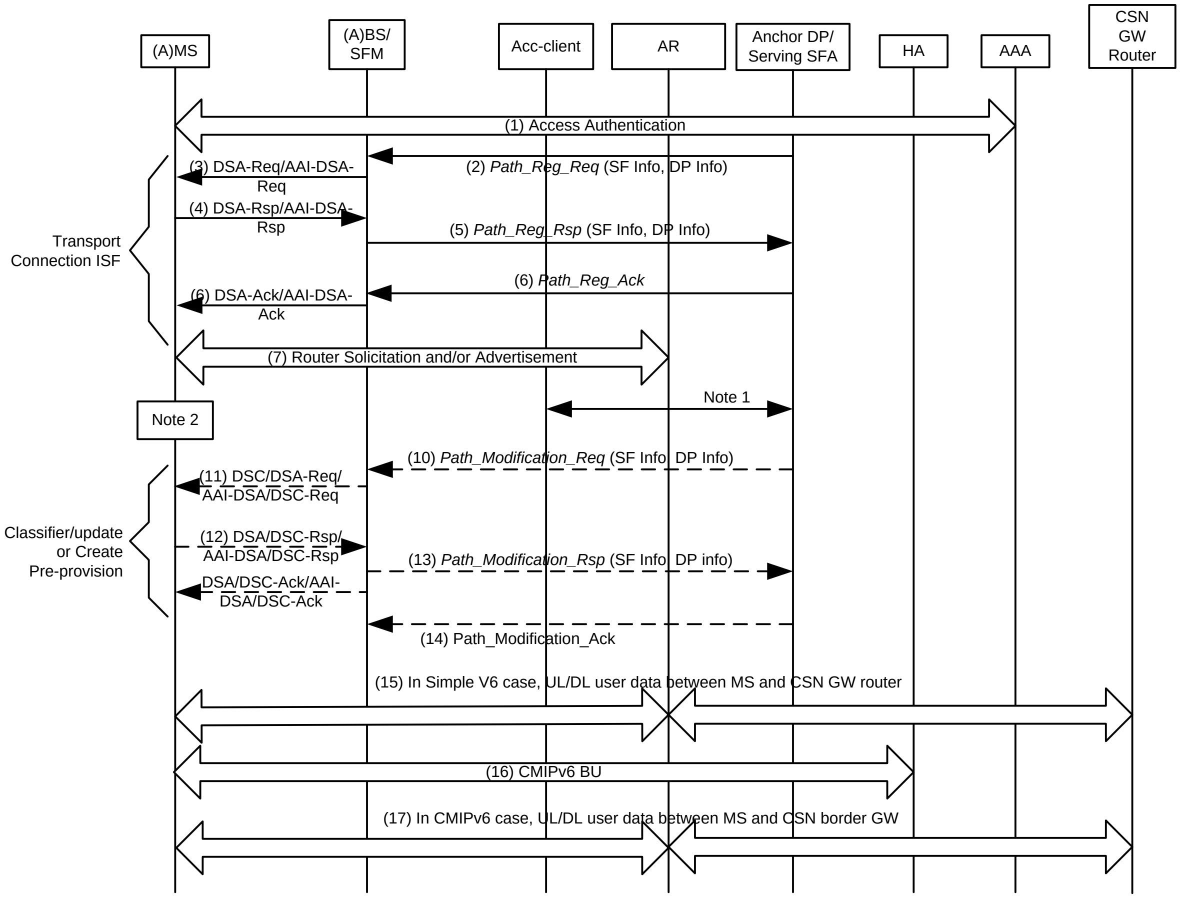
Since the ISF is established prior to the IP address assignment to the MS/AMS, the ASN cannot rely on the IP header information initially to determine the proper routing decision to forward any downlink traffic destined to the MS/AMS. Therefore, a special context binding, which contains the MSID and/or MS/AMS's NAI information, is required to be installed at the ASN to associate with the peer SFIDs of the ISF (i.e., the two unidirectional SFIDs for uplink and downlink) for the given MS/AMS to process the uplink and downlink IP packets. In the case when multiple pre-provisioning service flows including the ISF are established before the IP address assignment to the MS/AMS, for the IP CS based ISF, the special context binding may have to be done at the service flow level in order to allow the downlink IP client application signaling packet to be directed to the appropriate ISF transport over R6. During the time between initial creation of ISF and completion of IP address acquisition, all other pre-provisioned service flows SHALL not transport any IP traffic. The existence of the ISF does not preclude the MS to send IP configuration and IP client application signaling over another service flow that has been created by the MS/AMS once the MS/AMS has been assigned with an IP address with the support of ISF. Except from the time of creation, an ISF is treated like any other pre-provisioned service flow (like from the parameters settings as well as from the accounting perspective). Once the ASN is aware of the assigned IP address for the MS/AMS, ASN MAY perform the following steps:

- Update the classifier and QoS policy of the ISF, and any existing pre-provisioned service flow, which are created during the ISF.
- In the case where ISF was created and pre-provisioned flow was not created, ASN SHALL initiate the service flow creation request and apply the QoS policy to the pre-provisioned service flow.

Section 4.8, CSN Mobility Management supports four different IP address assignment mechanisms for the MS/AMS.

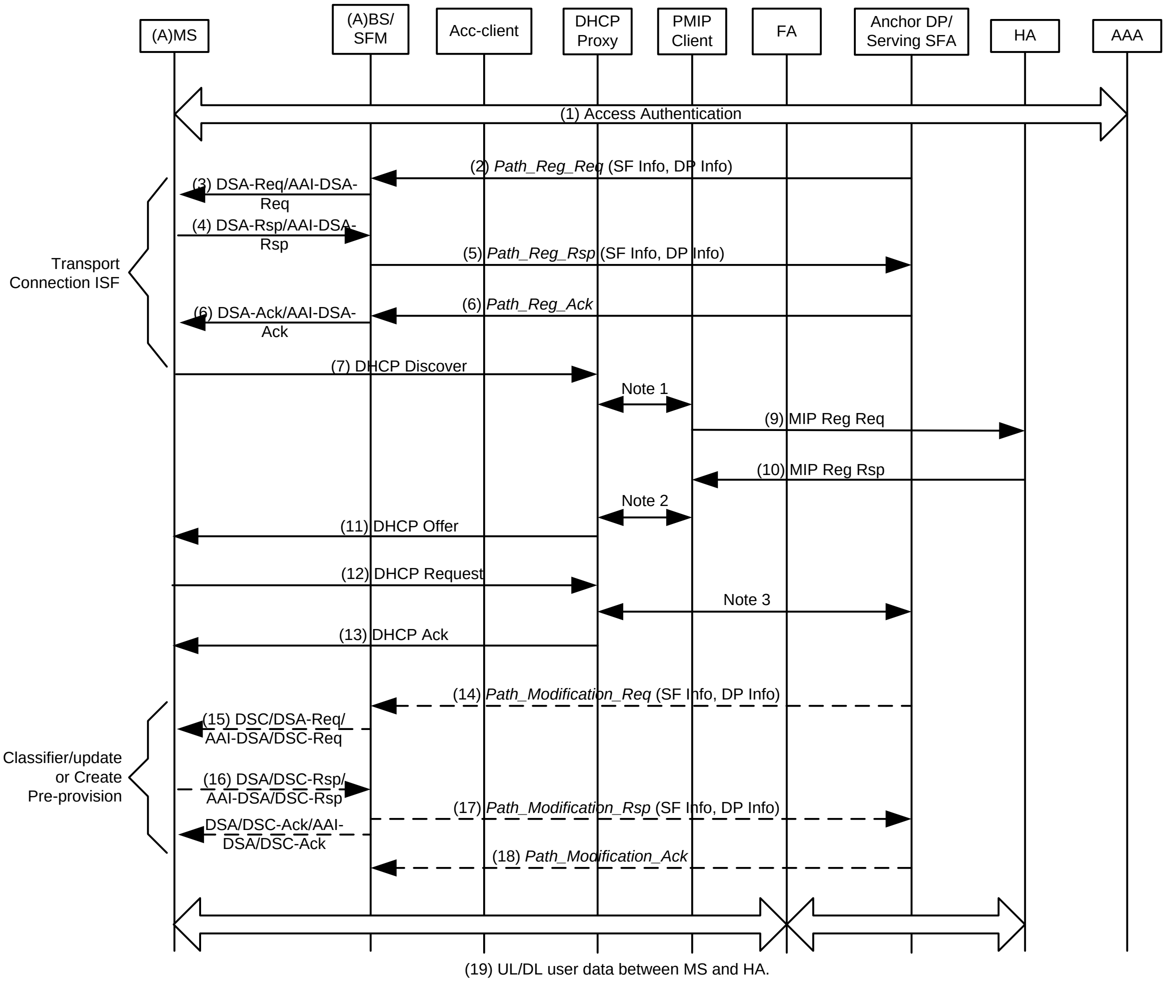
Figure 4-73, Figure 4-74, Figure 4-75 and Figure 4-76 show trigger and steps for updating the ISF and any existing pre-provision service flow for Simple IPv6/CMIP6, PMIP4, CMIP4 and for PMIP6 services in the respective order.

The purpose of the figures in this section is to contextualize the ISF data path setup with classifiers. The figures are informative. For further details, refer to the specific sections in this document.


(A)MS
(A)BS/ SFM
Acc-client
AR
Anchor DP/ Serving SFA
HA
AAA
CSN GW Router
(1) Access Authentication
(2) Path_Reg_Req (SF Info, DP Info)
(3) DSA-Req/AAI-DSA-Req
(4) DSA-Rsp/AAI-DSA-Rsp
(5) Path_Reg_Rsp (SF Info, DP Info)
Transport Connection ISF
(6) Path_Reg_Ack
(6) DSA-Ack/AAI-DSA-Ack
(7) Router Solicitation and/or Advertisement
Note 1
Note 2
(10) Path_Modification_Req (SF Info, DP Info)
(11) DSC/DSA-Req/ AAI-DSA/DSC-Req
Classifier/update or Create Pre-provision
(12) DSA/DSC-Rsp/ AAI-DSA/DSC-Rsp
(13) Path_Modification_Rsp (SF Info, DP info)
DSA/DSC-Ack/AAI-DSA/DSC-Ack
(14) Path_Modification_Ack
(15) In Simple V6 case, UL/DL user data between MS and CSN GW router
(16) CMIPv6 BU
(17) In CMIPv6 case, UL/DL user data between MS and CSN border GW

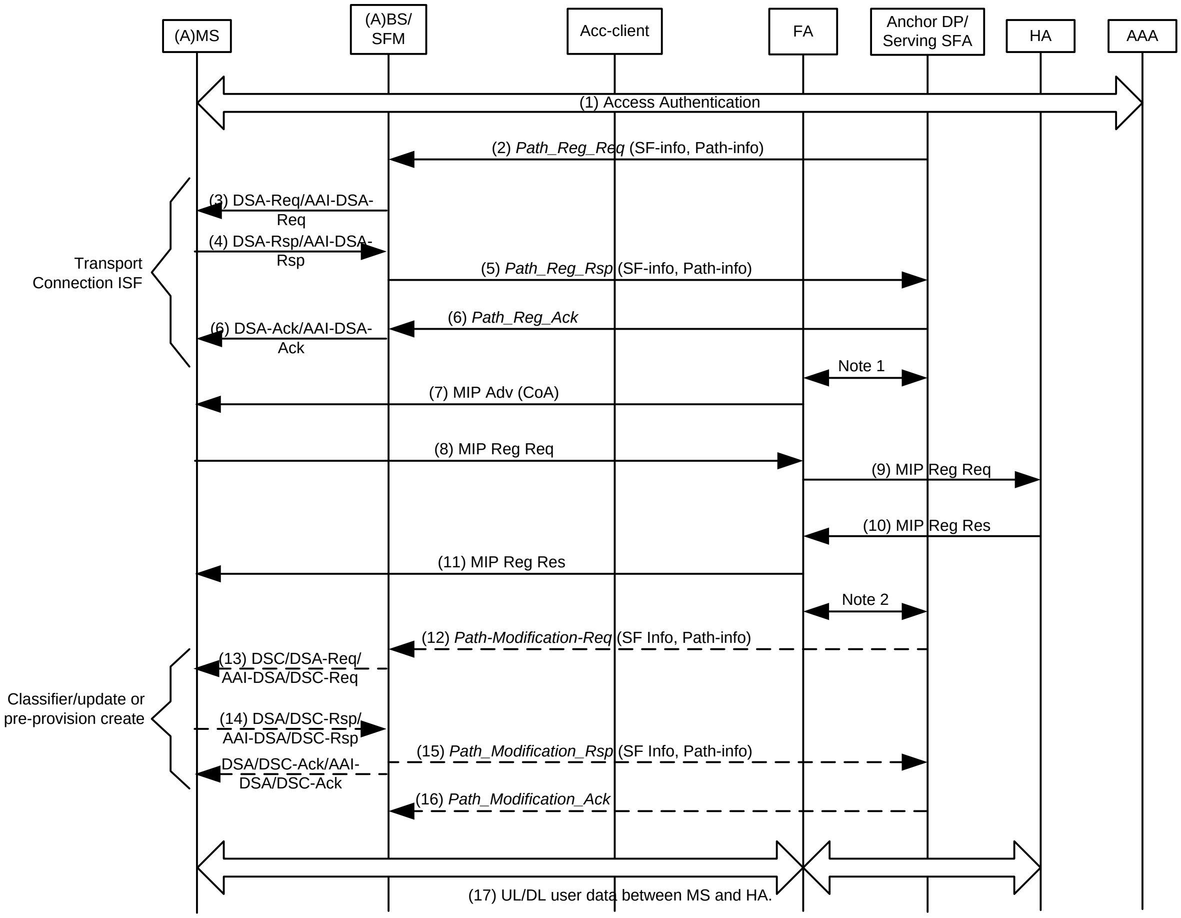
Note 1: AR in the ASN MAY trigger the Anchor DP/Serving SFA to update the SF classifier, with IPv6 Prefix (64bits).
At the same time, AR triggers ACC-Client to start Accounting-Start.
Note 2: Address Auto-configure and DAD occurs after the router solicitation, advertisement and DAD.

Figure 4-73 – ISF Classifier Update for IPv6


(A)MS
(A)BS/ SFM
Acc-client
DHCP Proxy
PMIP Client
FA
Anchor DP/ Serving SFA
HA
AAA
(1) Access Authentication
(2) Path_Reg_Req (SF Info, DP Info)
(3) DSA-Req/AAI-DSA-Req
(4) DSA-Rsp/AAI-DSA-Rsp
(5) Path_Reg_Rsp (SF Info, DP Info)
Transport Connection ISF
(6) DSA-Ack/AAI-DSA-Ack
(6) Path_Reg_Ack
(7) DHCP Discover
Note 1
(9) MIP Reg Req
(10) MIP Reg Rsp
Note 2
(11) DHCP Offer
(12) DHCP Request
Note 3
(13) DHCP Ack
(14) Path_Modification_Req (SF Info, DP Info)
(15) DSC/DSA-Req/ AAI-DSA/DSC-Req
Classifier/update or Create Pre-provision
(16) DSA/DSC-Rsp/ AAI-DSA/DSC-Rsp
(17) Path_Modification_Rsp (SF Info, DP Info)
DSA/DSC-Ack/AAI-DSA/DSC-Ack
(18) Path_Modification_Ack
(19) UL/DL user data between MS and HA.

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 4-74 – ISF Classifier Update for PMIP4

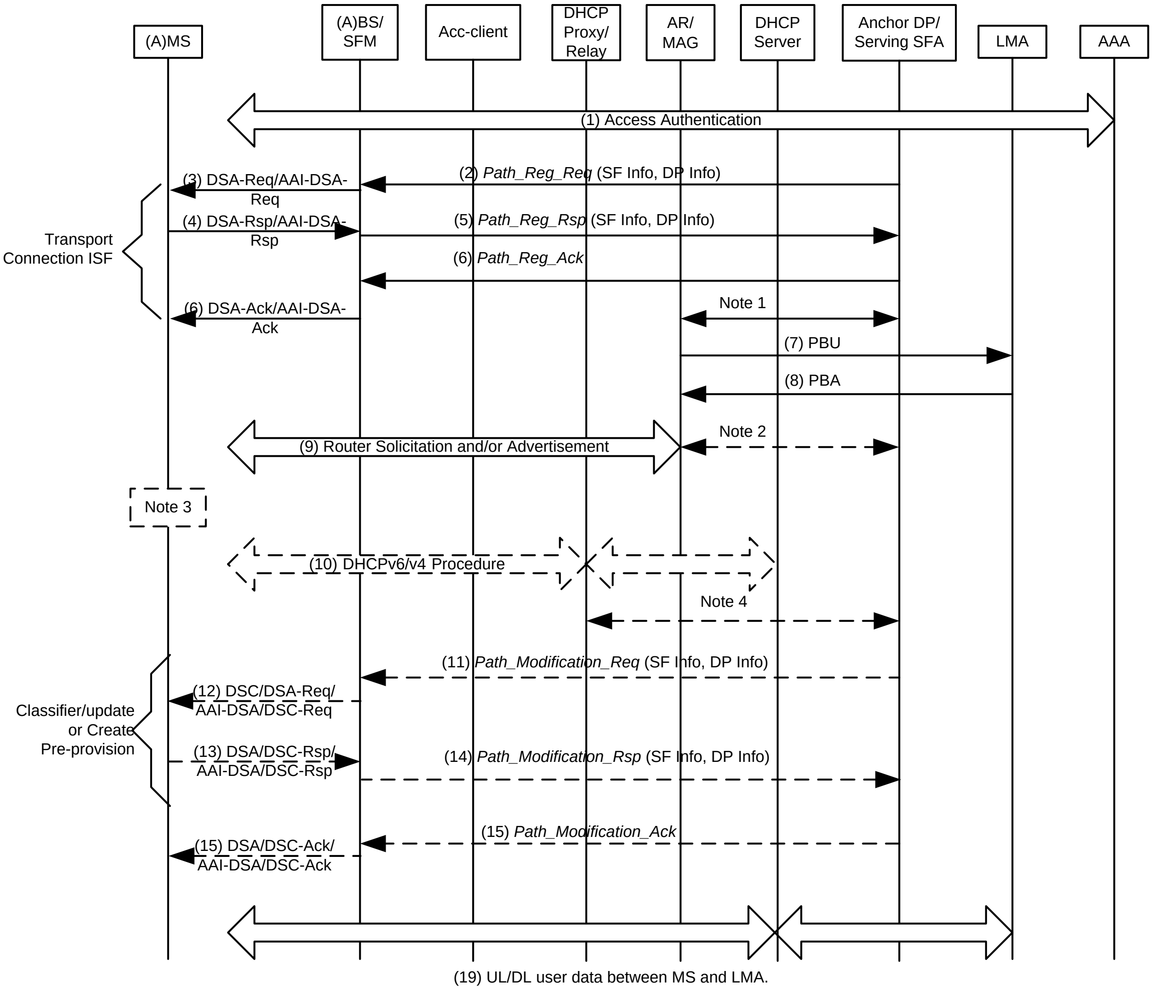

(A)MS
(A)BS/ SFM
Acc-client
FA
Anchor DP/ Serving SFA
HA
AAA
(1) Access Authentication
(2) Path_Reg_Req (SF-info, Path-info)
(3) DSA-Req/AAI-DSA-Req
(4) DSA-Rsp/AAI-DSA-Rsp
Transport Connection ISF
(5) Path_Reg_Rsp (SF-info, Path-info)
(6) Path_Reg_Ack
(6) DSA-Ack/AAI-DSA-Ack
Note 1
(7) MIP Adv (CoA)
(8) MIP Reg Req
(9) MIP Reg Req
(10) MIP Reg Res
(11) MIP Reg Res
Note 2
(12) Path-Modification-Req (SF Info, Path-info)
(13) DSC/DSA-Req/ AAI-DSA/DSC-Req
Classifier/update or pre-provision create
(14) DSA/DSC-Rsp/ AAI-DSA/DSC-Rsp
(15) Path_Modification_Rsp (SF Info, Path-info)
DSA/DSC-Ack/AAI-DSA/DSC-Ack
(16) Path_Modification_Ack
(17) UL/DL user data between MS and HA.

Note 1: Serving SFA triggers FA to initiate MIP registration (out of scope).
Note 2: FA in the ASN triggers the Anchor DP/Serving SFA to update the SF classifier (out of scope).

1

2 **Figure 4-75 – ISF Classifier Update for CMIP4**

3


(A)MS
(A)BS/ SFM
Acc-client
DHCP Proxy/ Relay
AR/ MAG
DHCP Server
Anchor DP/ Serving SFA
LMA
AAA
(1) Access Authentication
(2) Path_Reg_Req (SF Info, DP Info)
(3) DSA-Req/AAI-DSA-Req
(4) DSA-Rsp/AAI-DSA-Rsp
(5) Path_Reg_Rsp (SF Info, DP Info)
(6) Path_Reg_Ack
Transport Connection ISF
(6) DSA-Ack/AAI-DSA-Ack
Note 1
(7) PBU
(8) PBA
(9) Router Solicitation and/or Advertisement
Note 2
Note 3
(10) DHCPv6/v4 Procedure
Note 4
(11) Path_Modification_Req (SF Info, DP Info)
(12) DSC/DSA-Req/ AAI-DSA/DSC-Req
Classifier/update or Create Pre-provision
(13) DSA/DSC-Rsp/ AAI-DSA/DSC-Rsp
(14) Path_Modification_Rsp (SF Info, DP Info)
(15) Path_Modification_Ack
(15) DSA/DSC-Ack/ AAI-DSA/DSC-Ack
(19) UL/DL user data between MS and LMA.

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 4-76 – ISF Classifier Update for PMIP6

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.

In the case of ETH CS, the QoS profile of a service flow MAY contain additional information for the processing of VLAN tags. The TLVs for VLAN tag processing are defined in chapter 5 of this document.

4.6.4.2.2.1 Prioritization for Ethernet Services

The user_priority field in the VLAN Tag can be used to mark the particular QoS class of Ethernet frames in the wired part of the WiMAX network. User_priority, if present is usually set at the entry to the network and MAY be used by network elements along the path for control of the treatment of the frames in the forwarding process.

The Layer 2 Forwarding (L2FW) function in the ASN-GW SHALL support the assignment of the priority bits in the VLAN tag in upstream and downstream direction for each service flow dependent of the QoS profile provisioned by the AAA server. The assignment of the priority bits SHALL follow one of three ways listed below:

- Forward the frame without modification of the priority bits
- Set the priority bits to a value provided by the AAA server as part of the SF specification
- Restrict the usage of a higher priority than signaled by the AAA server as part of the SF specification.
    - Frames with priorities higher than allowed SHALL either be remarked to the highest allowed value or be dropped.

If assignment of the priority_field in the VLAN tag is enforced for a particular service flow, the L2FW function SHALL insert VLAN tags with VLAN ID and priority field set to the specified values into Ethernet frames without VLAN tags belonging to the service flow.

4.6.4.2.2.2 VLAN Tag Processing for Ethernet Services

VLAN-IDs are used in many different ways for segregating traffic of Ethernet services in the access network. The L2FW function in the ASN-GW SHALL support the flexible use of the VLAN-IDs by providing the following capabilities for each of the service flows:

The configuration information of the VLAN tag processing SHALL be provided by the AAA server as part of the SF specification.

In downstream direction towards the MS:

- The L2FW SHALL be able to remove S-VLAN tags or C-VLAN tags if present. The VLAN tags SHALL be removed after making use of the VLAN tag for classification purposes.

In upstream direction from the MS:

- The L2FW SHALL be able to add S-VLAN tags to Ethernet frames containing a C-VLAN tag. The inserted S-VIDs may be either set to a fixed value or assigned depending of the C-VID according to a mapping table provided by the AAA server as part of the SF specification. The priority bits SHALL be either set to a fixed value provided by the AAA server as part of the SF specification or copied from the priority bits in the C-VLAN tag.
- The L2FW SHALL be able to insert VLAN tags with an assigned C-VID into Ethernet frames without VLAN tagging. The C-VID value and the priority bits are provided as part of the SF specification by the AAA server.

Service flows belonging to a MS SHALL inherit the VLAN tag processing behavior of the ISF when nothing is specified for the particular service flow but a specification is provided for the ISF.

For local configuration a string MAY be provided for local use together with the configuration information of the VLANTagProcessing.

Note: The string provided together with the configuration information of the VLANTagProcessing may be used e.g. for configuration of the R3 data path for other transport protocols like MPLS or IEEE 802.1ah (MAC-in-MAC) in the case of Simple Ethernet.

Note: VLANTagProcessing configuration is part of the packet flow descriptor, which can be pre-configured locally. The means to provide the local configuration data is out of scope of this specification.

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 or a bi-directional flow. A PD-flow is bound to a single WiMAX service flow when PDFID represents a unidirectional flow; and two service flows when PDFID represents a bi-directional 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/AMS – 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/AMS's subscription profile that is downloaded from the H-AAA or V-AAA after the successful MS/AMS access authentication as well as dependent on the local BS/ABS'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/AMS is attached to the ASN. However, if any of the ISFs fails to be supported by the local ASN, the MS/AMS 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/AMS 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/AMS.

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.

4.6.4.2.7 Dual Stack MS/AMS and Dual Stack Network Related Issue

After successful authentication, MS/AMS and network negotiate CS capability via registration procedure. Once ASN knows that MS/AMS is dual stacked and CSN permits simultaneous IPv4 and IPv6 registration, ASN-GW will trigger two independent ISF establishment procedures respectively for IPv4 and IPv6. Then, if the two ISF pairs are established, MAG on ASN-GW shall trigger a PBU message to LMA for simultaneous IPv4 and IPv6 registration. There is no need to wait for DHCPDISCOVER message to trigger PBU for dual stack MS/AMS.

Each ISF shall include one uplink and one downlink service flow. Both ISFs must be established before the BS/ABS establishes any other SFs to the MS/AMS.

The number of ISFs to be established is detemined by the MS/AMS based on the IP-CS support as defined in the REG-RSP, e.g. if both IPv4-CS and IPv6-CS are supported by MS/AMS and required by network, two ISF pairs shall be created.

Following that, DHCPv4 procedure can happen as well as DHCPv6 procedure.

Procedure is shown in Figure 4-77.

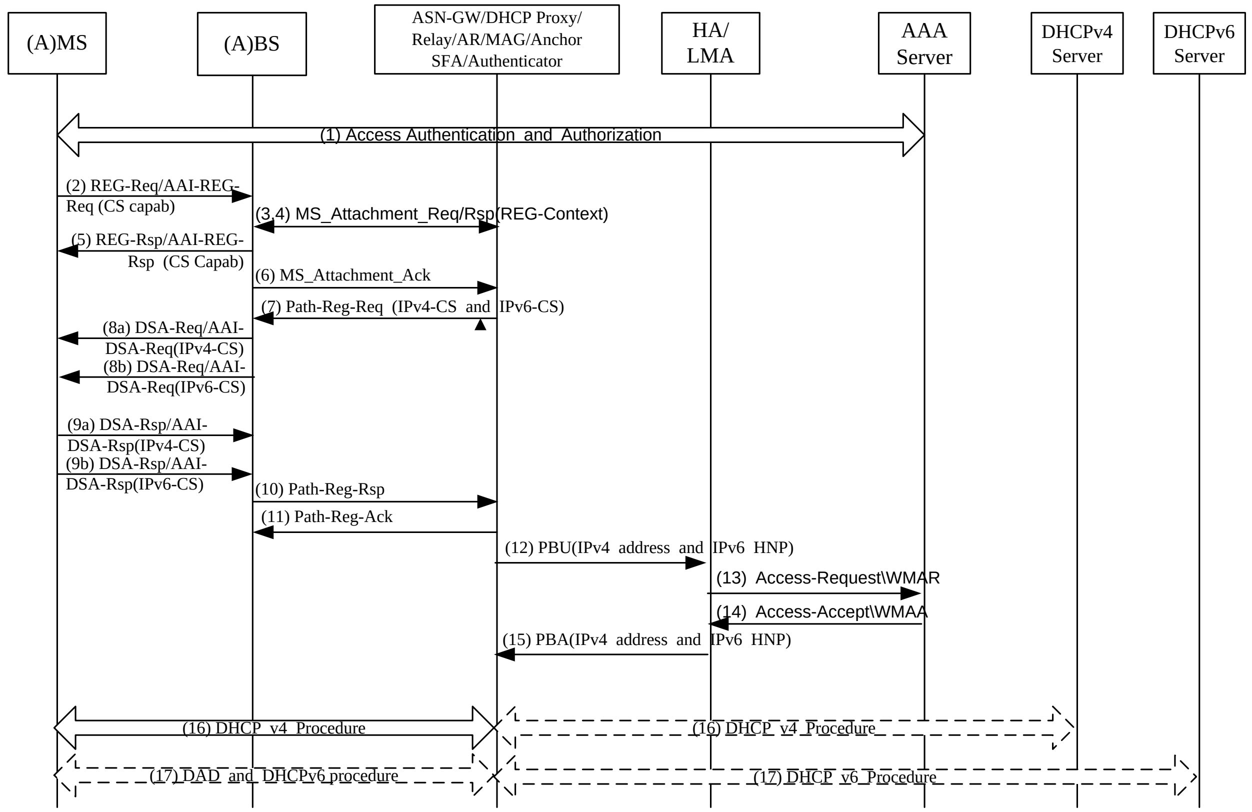

(A)MS
(A)BS
ASN-GW/DHCP Proxy/ Relay/AR/MAG/Anchor SFA/Authenticator
HA/ LMA
AAA Server
DHCPv4 Server
DHCPv6 Server
(1) Access Authentication and Authorization
(2) REG-Req/AAI-REG-Req (CS capab)
(3,4) MS_Attachment_Req/Rsp (REG-Context)
(5) REG-Rsp/AAI-REG-Rsp (CS Capab)
(6) MS_Attachment_Ack
(7) Path-Reg-Req (IPv4-CS and IPv6-CS)
(8a) DSA-Req/AAI-DSA-Req(IPv4-CS)
(8b) DSA-Req/AAI-DSA-Req(IPv6-CS)
(9a) DSA-Rsp/AAI-DSA-Rsp(IPv4-CS)
(9b) DSA-Rsp/AAI-DSA-Rsp(IPv6-CS)
(10) Path-Reg-Rsp
(11) Path-Reg-Ack
(12) PBU(IPv4 address and IPv6 HNP)
(13) Access-Request\WMAR
(14) Access-Accept\WMAA
(15) PBA(IPv4 address and IPv6 HNP)
(16) DHCP v4 Procedure
(16) DHCP v4 Procedure
(17) DAD and DHCPv6 procedure
(17) DHCP v6 Procedure

Figure 4-77 – ISF establishment for DS MS/AMS and network

STEP 1

This is access authentication and authorization procedure. The QoS Profile is optionally provided to the NAS function in the ASN-GW.

STEP 2

MS/AMS provides its CS Capability in *REG-REQ/AAI-REG-REQ*.

STEP 3

MS/AMS Attachment Request forwards the REG Context to the ASN-GW.

STEP 4

ASN-GW compares the CS capability from MS/AMS with the Network Service Capability (see 4.4.1.5) downloaded from AAA Server and makes decision on allowed CS capability for MS/AMS (CS capability is allowed if it was both requested by the MS/AMS and affirmed by the AAA). The ASN-GW then formulates a new REG Context and uses MS/AMS Attachment Response to forward the negotiated REG Context to the BS/ABS.

STEP 5

BS/ABS responds with *REG-RSP/AAI-REG-RSP* indicating the ASN CS Capability.

STEP 6

BS/ABS responds to NAS with *MS/AMS Attachment Ack*.

STEP 7

Anchor SFA initiates DP(s) per provided QoS profile and REG Context. In case no profile is provided and hot-lining is used, a_SFA initiates only IPv4 DP for hot-lining. If IPv4 and IPv6 are both supported by MS/AMS and network as allowed in the CS capability negotiation of step 4, then the related QoS information for establishing IPv4 and IPv6 ISFs shall be included as specified in section 4.6.5.4.1.

STEP 8

8a. BS/ABS sends *DSA-REQ/AAI-DSA-REQ* to MS/AMS by including the related QoS information for establishing IPv4-CS ISF.

8b. BS/ABS sends *DSA-REQ/AAI-DSA-REQ* to MS/AMS by including the related QoS information for establishing IPv6-CS ISF.

Step 8a and 8b can happen in parallel.

STEP 9

9a. MS/AMS responds to BS/ABS with *DSA-RSP/AAI-DSA-RSP* for IPv4-CS.

9b. MS/AMS responds to BS/ABS with *DSA-RSP/AAI-DSA-RSP* for IPv6-CS.

Step 9a and 9b can happen in parallel.

STEP 10

When receiving *DSA-RSP/AAI-DSA-RSP*, BS/ABS responds to Anchor SFA with *Path-Reg-Rsp* as specified in section 4.6.5.4.1.

STEP 11

Anchor SFA responds to BS/ABS with *Path-Reg-Ack* as specified in section 4.6.5.4.1.

STEP 12

The AR/MAG in ASN 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 IPv4-HoA and HNP were obtained from the HAAA, this information populates Home-IPv4-HoA-PMIP6 and Home-HNP-PMIP6 included in the PBU.

STEP 13

After receiving the PBU message (message composition in section 4.8.5.3.3), the LMA initiates Authorization of MAG ASN 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 14

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/AMS’s PMIP6 session. LMA creates the tunnel(s) towards the AR/MAG ASN and sets the routing rule directing all packets destined to the IPv4-HoA and all packets destined to HNP via the established PMIP6 tunnel(s).

STEP 15

The LMA sends the PBA to the AR/MAG ASN to confirm the initial binding registration and invokes creation of the dynamic bi-directional PMIP6 tunnel(s) for MS/AMS’s uplink and downlink payload forwarding. The PBA includes the MS/AMS’s assigned IPv4-HoA and the prefix in the HNP option, has the HO indicator value set to one (HOI=1), the Access Technology Type (ATT) option set to a value five, and the Link-local option populated as described in section 4.8.5.3.5.

STEP 16

DHCPv4 procedures. If DHCPv4 Proxy is enabled, there is no interaction between the ASN-GW and the DHCPv4 Server.

STEP 17

Optional DAD and DHCPv6 procedures for stateful IPv6 address configuration; Optional DAD and Router Solicitation/Advertisement for steteless IPv6 address configuration. If DHCPv6 Proxy is enabled, there is no interaction between ASN-GW and DHCPv6 Server.

- Note 1: If CS capability between MS/AMS and ASN is completely mismatched, step 5 is changed to *DREG-REQ*.
- Note 2: Step 16 and 17 are independent of each other and can be executed in parallel.
- Note 3: Steps 16 and 17 can happen after step 9.

4.6.4.3 Default Service Flow

Default Service Flow (DSF) is a pair of special service flows (one uplink and one downlink service flow) which shall be automatically established during AMS initial network entry at the MZone of an ABS.

The QoS parameters set of the DSF is pre-defined by the IEEE802.16m [105] and the operator policy, and is independent of each individual AMS. After successful transaction of AAI-REG-REQ/RSP between ABS and AMS, the DSF shall be created and activated at the network and AMS, using the pre-provisioned QoS parameters values, without further signaling message transactions to set up a service flow.

If the DSF could not be successfully set up during the initial network entry of an AMS, the AMS SHALL be denied of the service by the local ASN.

If the DSF is successfully established by the AMS and the network, it shall be used as the ISF, that is, the first active service flow 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.

In case that multiple CS types are activated at the same time by the AMS and the ASN, the CS type for the DSF shall be decided by the ASN based on the operator policy information stored at the ASN, and shall be informed to the AMS using the AAI-REG-RSP message during the AMS initial network entry.

The ISFs for the other CS types which do not use the DSF, can be activated successfully for the MS/AMS by complying with the procedures defined in sec. 4.6.4.2.

The number of retries for the local ASN to attempt to establish the DSF is local network policy decision and is outside the scope of this specification.

Figure 4-78 and Figure 4-79 shows the procedure for initializing the ISF through the setup of the DSF.

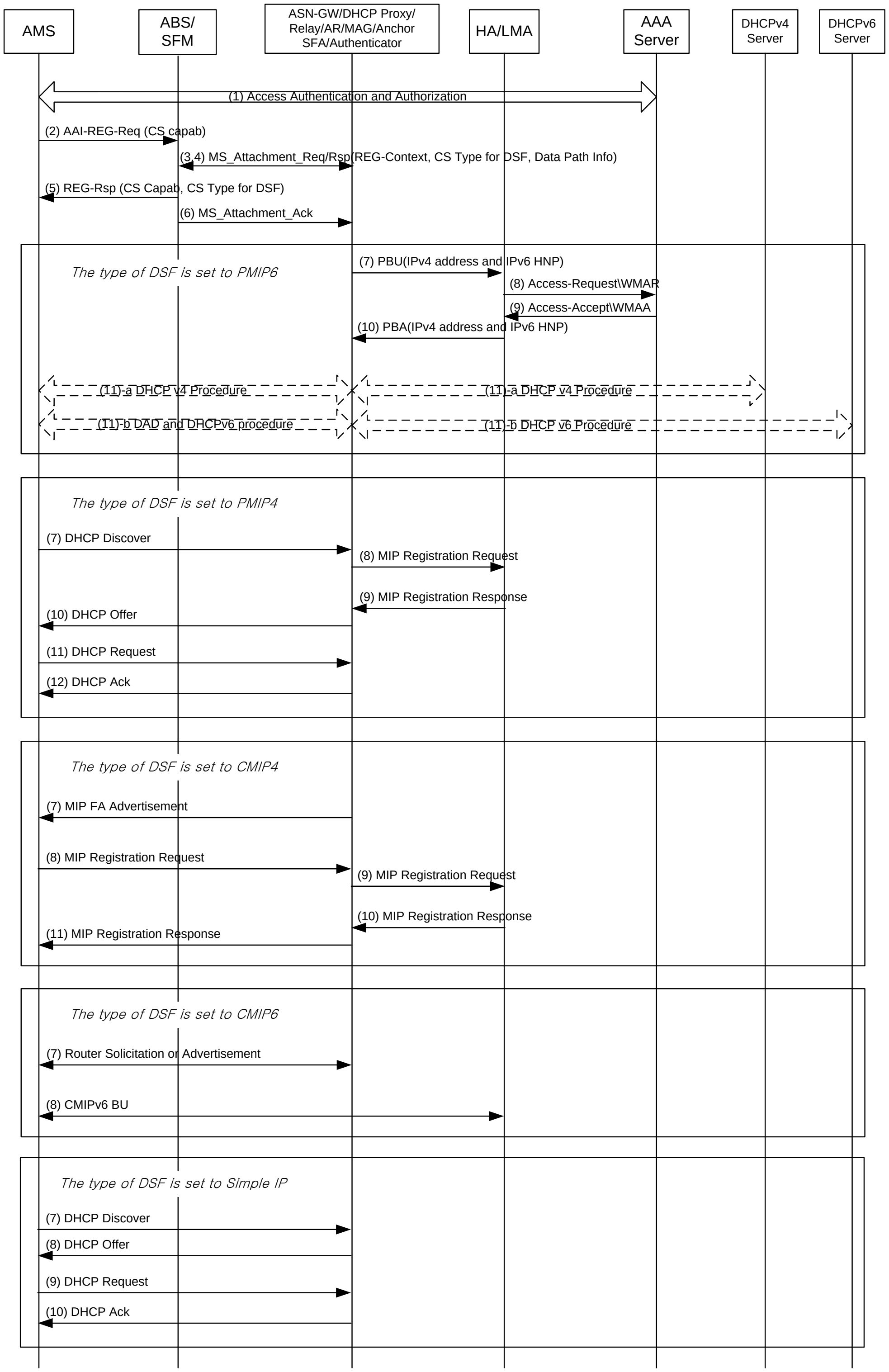

AMS
ABS/ SFM
ASN-GW/DHCP Proxy/ Relay/AR/MAG/Anchor SFA/Authenticator
HA/LMA
AAA Server
DHCPv4 Server
DHCPv6 Server
(1) Access Authentication and Authorization
(2) AAI-REG-Req (CS capab)
(3,4) MS_Attachment_Req/Rsp (REG-Context, CS Type for DSF, Data Path Info)
(5) REG-Rsp (CS Capab, CS Type for DSF)
(6) MS_Attachment_Ack
The type of DSF is set to PMIP6
(7) PBU(IPv4 address and IPv6 HNP)
(8) Access-Request\WMAR
(9) Access-Accept\WMAA
(10) PBA(IPv4 address and IPv6 HNP)
(11)-a DHCP v4 Procedure
(11)-a DHCP v4 Procedure
(11)-b DAD and DHCPv6 procedure
(11)-b DHCP v6 Procedure
The type of DSF is set to PMIP4
(7) DHCP Discover
(8) MIP Registration Request
(9) MIP Registration Response
(10) DHCP Offer
(11) DHCP Request
(12) DHCP Ack
The type of DSF is set to CMIP4
(7) MIP FA Advertisement
(8) MIP Registration Request
(9) MIP Registration Request
(10) MIP Registration Response
(11) MIP Registration Response
The type of DSF is set to CMIP6
(7) Router Solicitation or Advertisement
(8) CMIPv6 BU
The type of DSF is set to Simple IP
(7) DHCP Discover
(8) DHCP Offer
(9) DHCP Request
(10) DHCP Ack

Figure 4-78 – ISF Establishment using Defaul SF(without FIAA)

STEP 1

AMS performs Access Authentication and Authorization with AAA server. The QoS Profile is optionally provided to the NAS function in the ASN-GW by AAA.

STEP 2

AMS provides its CS Capability in an *AAI-REG-REQ* message.

STEP 3

ABS forwards the REG Context in an MS_Attachment_Request message to the ASN-GW. ABS includes the Data Path information for the GRE tunnel which is to identify the R6 data path for the DSF.

STEP 4

ASN-GW compares the CS capability received from AMS with the Network Service Capability (see 4.4.1.6) downloaded from the AAA Server and makes decision on allowed CS capability for the AMS (CS capability is allowed if it was both requested by the AMS and affirmed by the AAA). The ASN GW also selects one CS type of the allowed CS capability to use for Default Service Flow (DSF), based on the operator policy information which may be locally stored at the ASN GW or provided by the AAA server during the access authentication procedure.

The ASN-GW then formulates a new REG Context which includes the allowed CS capability, the selected CS type for DSF, and Data Path ID for the DSF. The ASN GW sends an MS_Attachment_Response message to forward the negotiated REG Context to the ABS.

STEP 5

ABS responds to AMS with an *AAI-REG-RSP* message including the agreed CS Capability.

ABS shall establish the DSF for the specified CS type, using the pre-defined SFID, QoS parameter sets, classification rules, scheduling type, etc.

Upon receiving the *AAI-REG-RSP* message, the AMS shall create the DSF with the provided SFID, QoS parameters sets, classification rules, scheduling type, etc.

STEP 6

ABS responds to NAS with *MS/AMS Attachment Ack* which includes Data Path Info for downlink traffic of the DSF.

The ISF setup procedure for the IP Mobility scheme specified for the AMS follows:

i) PMIP6

STEP 7 – STEP 11

Upon receiving the MS_Attachment_Request, the AR/MAG for PMIP6 (Anchor SFA) initiates the initial binding registration (PBU/PBA) procedure, which in turn triggers the Access-Request/Response transaction between the HA and the AAA server.

Refer to STEP 12-17 of Figure 4-77, for detailed operations.

ii) PMIP4

STEP 7 – STEP 12

After setting up the DSF, the AMS performs DHCP procedure with DHCP proxy at the ASN GW which in turn initiates MIP Registration procedure with HA.

Refer to STEP 7-13 of Figure 4-74, for detailed operations.

iii) CMIP4

STEP 7 – STEP 11

Upon receiving the MS_Attachment_Request, the FA at the ASN GW sends MIP Router Advertisement message to the AMS to initiate MIP Registration procedure. AMS starts MIP Registration with the HA specified in the received MIP Router Advertisement message.

Refer to STEP 7-11 of Figure 4-75, for detailed operations.

iv) CMIP6

STEP 7 – STEP 8

Upon receiving the MS_Attachment_Request, the FA at the ASN GW sends MIP Router Advertisement message to the AMS to initiate MIP Registration procedure. AMS starts MIP Registration with the HA specified in the received MIP Router Advertisement message.

Refer to STEP 7-11 of Figure 4-75, for detailed operations.

v) Simple IP

STEP 7 – STEP 10

After setting up the DSF, the AMS performs DHCP procedure with DHCP proxy at the ASN GW.

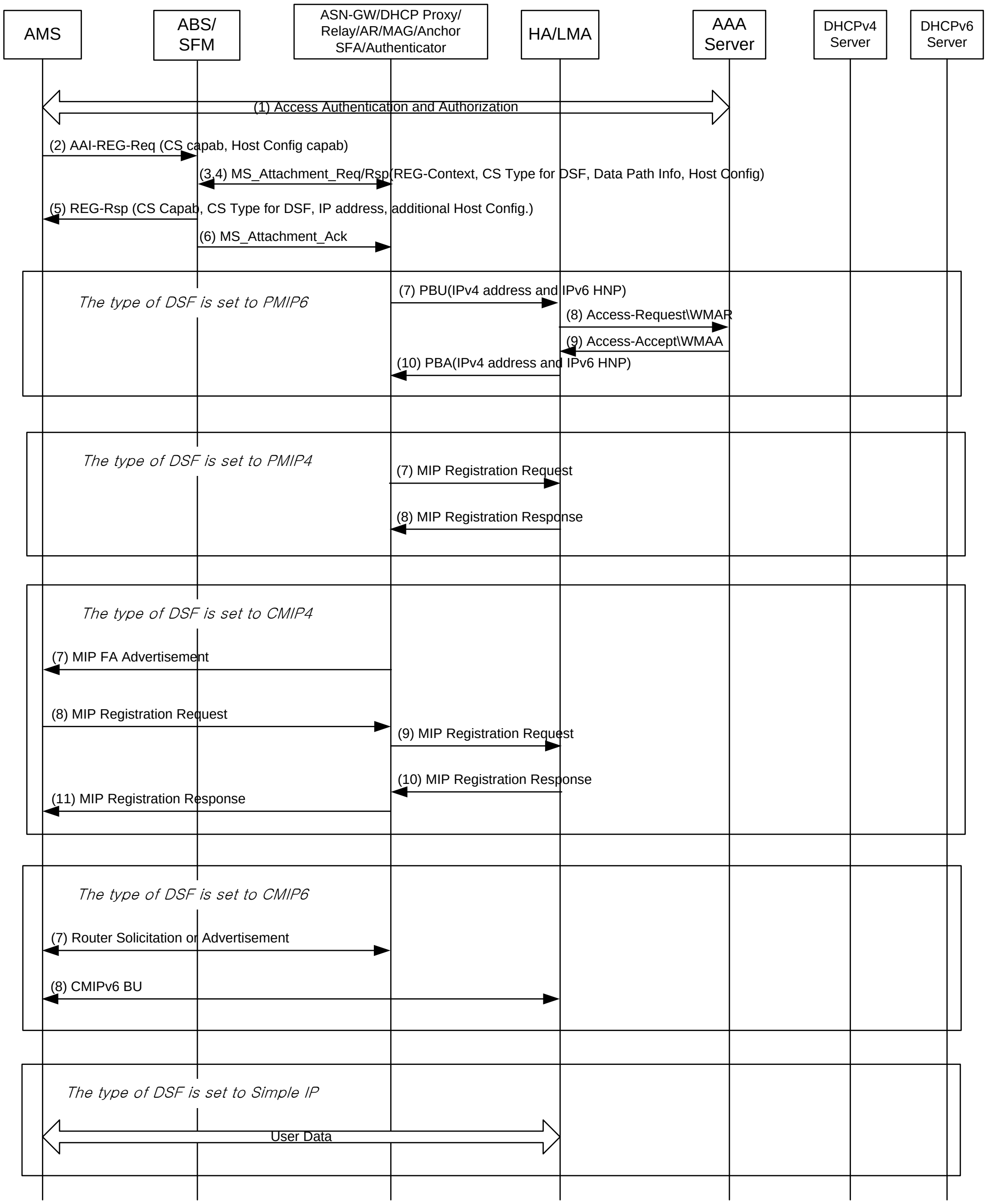

AMS
ABS/ SFM
ASN-GW/DHCP Proxy/ Relay/AR/MAG/Anchor SFA/Authenticator
HA/LMA
AAA Server
DHCPv4 Server
DHCPv6 Server
(1) Access Authentication and Authorization
(2) AAI-REG-Req (CS capab, Host Config capab)
(3,4) MS_Attachment_Req/Rsp(REG-Context, CS Type for DSF, Data Path Info, Host Config)
(5) REG-Rsp (CS Capab, CS Type for DSF, IP address, additional Host Config.)
(6) MS_Attachment_Ack
The type of DSF is set to PMIP6
(7) PBU(IPv4 address and IPv6 HNP)
(8) Access-Request\WMAR
(9) Access-Accept\WMAA
(10) PBA(IPv4 address and IPv6 HNP)
The type of DSF is set to PMIP4
(7) MIP Registration Request
(8) MIP Registration Response
The type of DSF is set to CMIP4
(7) MIP FA Advertisement
(8) MIP Registration Request
(9) MIP Registration Request
(10) MIP Registration Response
(11) MIP Registration Response
The type of DSF is set to CMIP6
(7) Router Solicitation or Advertisement
(8) CMIPv6 BU
The type of DSF is set to Simple IP
User Data

Figure 4-79 – ISF Establishment using Defaul SF(with FIAA)

STEP 1

AMS performs Access Authentication and Authorization with AAA server. The QoS Profile is optionally provided to the NAS function in the ASN-GW by the AAA.

STEP 2

AMS provides its CS Capability and Host Configuration Capability, which indicates that the AMS supports FIAA feature, in an AAI-REG-REQ message.

STEP 3

ABS forwards the REG Context in an *MS_Attachment_Request* message to the ASN-GW. ABS includes the Data Path information for the GRE tunnel which is to identify the R6 data path for the DSF.

STEP 4

ASN-GW compares the CS capability received from AMS with the Network Service Capability (see 4.4.1.6) downloaded from the AAA Server and makes decision on allowed CS capability for the AMS (CS capability is allowed if it was both requested by the AMS and affirmed by the AAA). The ASN GW also selects one CS type of the allowed CS capability to use for Default Service Flow (DSF), based on the operator policy information which may be locally stored at the ASN GW or provided by the AAA server during the access authentication procedure.

If the Host Configuration Capability, which is received from the ABS, is set to 1, the DHCP Proxy/Relay function at the ASN GW performs the IP address assignment procedure for the AMS.

The ASN-GW then formulates a new REG Context TLV which includes the allowed CS capability, the selected CS type for DSF, the assigned HoA (for IPv4) or the assigned HNP (for IPv6), and Data Path ID for the DSF. The ASN GW sends an *MS_Attachment_Response* message to forward the negotiated REG Context to the ABS.

STEP 5

ABS responds to AMS with an AAI-REG-RSP message including the agreed CS Capability.

ABS shall establish the DSF for the specified CS type, using the pre-defined SFID, QoS parameter sets, classification rules, scheduling type, etc.

Upon receiving the AAI-REG-RSP message, the AMS shall create the DSF with the provided SFID, QoS parameters sets, classification rules, scheduling type, etc.

STEP 6

ABS responds to NAS with *MS_Attachment Ack* which includes Data Path Info for downlink traffic of the DSF.

The ISF setup procedure for the IP Mobility scheme specified for the AMS follows:

i) PMIP6

STEP 7 – STEP 11

Upon receiving the MS_Attachment_Request, the AR/MAG for PMIP6 (Anchor SFA) initiates the initial binding registration (PBU/PBA) procedure, which in turn triggers the Access-Request/Response transaction between the HA and the AAA server.

Refer to STEP 12-17 of Figure 4-77, for detailed operations.

ii) PMIP4

STEP 8 – STEP 13

After setting up the DSF, the AMS performs DHCP procedure with DHCP proxy at the ASN GW which in turn initiates MIP Registration procedure with HA.

Refer to STEP 7-13 of Figure 4-74, for detailed operations.

iii) CMIP4

STEP 9 – STEP 11

Upon receiving the MS_Attachment_Request, the FA at the ASN GW sends MIP Router Advertisement message to the AMS to initiate MIP Registration procedure. AMS starts MIP Registration with the HA specified in the received MIP Router Advertisement message.

Refer to STEP 7-11 of Figure 4-75, for detailed operations.

iv) Simple IP

Upon receiving the MS_Attachment_Request, the FA at the ASN GW sends MIP Router Advertisement message to the AMS to initiate MIP Registration procedure. AMS starts MIP Registration with the HA specified in the received MIP Router Advertisement message.

Refer to STEP 7-11 of Figure 4-75, for detailed operations.

Table 4-58 and Table 4-59 shows the required changes for MS_Attachment_Req and MS_Attachment_Rsp message respectively.

Table 4-58 – 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.
>SF Info	5.3.2.185	O	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.
>> Data Path Info	5.3.2.45	CM	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.
>>> Data Path ID	5.3.2.44	CM	Specifies the data path for default service flow.
>>> Tunnel Endpoint	5.3.2.194	O	
> 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	O	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	O	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	O	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	O	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum MAC Data per Frame Support	5.3.2.296	O	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	O	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	O	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	O	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	

IE	Reference	M/O	Notes
> 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 **Table 4-59 – 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.
> CS specification for default service flow	5.3.2.501	O	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.
> SF Info	5.3.2.185	O	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.
>> Data Path Info	5.3.2.45	CM	SHALL be included if AMS sent REG-REQ at the MZone of the ABS.
>>> Data Path ID	5.3.2.44	CM	Specifies the data path for default service flow.
>>> Tunnel Endpoint	5.3.2.194	O	
> REG Context	5.3.2.144	O	Identifies the MS REG Context parameters as enforced by the Authenticator. SHALL be included if it in include 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	O	This TLV SHALL be included if REG Context is included in the transmitted message.
>>Maximum Number of Classifier	5.3.2.291	O	This TLV SHALL be included if REG Context is included in the transmitted message.
>>PHS Support	5.3.2.292	O	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	O	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	

IE	Reference	M/O	Notes
>>Maximum MAC Data per Frame Support	5.3.2.296	O	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	O	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	O	This TLV SHALL be included if REG Context is included in the transmitted message.
>>ARQ Ack Type	5.3.2.307	O	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.

IE	Reference	M/O	Notes
>>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	

4.6.4.3.1 Create Service Flow

The Default Service Flow 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. During the initial network entry procedure, the CS type for the DSF shall be decided by the ASN and be known to the AMS. The DSF does not use the explicit signaling messages to set up, but relies on the attachment procedure during the network entry. The ASN shall piggyback necessary information to set up the DSF in the attachment response message. The SFID of the DSF shall be reserved as ‘0x0011’ for both uplink and downlink directions at the ASN and the AMS. Upon successful reception of the AAI-REG- RSP message, the AMS shall create and activate the DSF for the specified CS type using the pre-provisioned QoS parameter values.

4.6.4.3.2 Delete Service Flow

The Default Service Flow shall be set as the ISF for the CS type which is selected by the ASN during the network entry for the AMS, and shall be treated the same through the AMS WiMAX session as the ISFs for the other CS types which are set up without using the DSF. Therefore, deletion of the DSF can take place as part of the network exit procedure, as specified in section 4.6.4.2.5.

4.6.4.3.3 Modify Service Flow

A modification of the DSF may be necessary if an ASN creates the DSF using the default QoS parameter values which need to be adapted according to the QoS profile received from the home CSN after the allocation of an IP-address. As in the case of the ISF, the HAAA may request the modification of the current QoS profile for the DSF present in the ASN. In such a case, the existing DSF, which is being used as one of the ISF, may require to be updated because of changed QoS parameters.

4.6.4.4 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.

4.6.4.4.1 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/AMS 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/AMS 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.

4.6.4.4.2 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/AMS. 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.

4.6.4.4.3 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/AMS 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.

4.6.4.5 Data Path Handling

The serving SFA SHALL trigger the establishment of the Data Path. The creation per SF SHALL be mandatorily supported.

4.6.4.6 Message Flows and Flow Description

4.6.4.6.1 Update of Pre-Provisioned QoS triggered by AAA

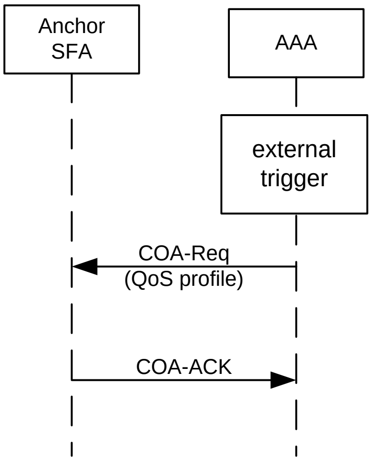


Figure 4-80 – AAA-Triggered QoS Profile update

Corresponding COA messages are defined in 5.4.1.8.

4.6.4.6.2 Network Initiated Service Flow Creation/Modification

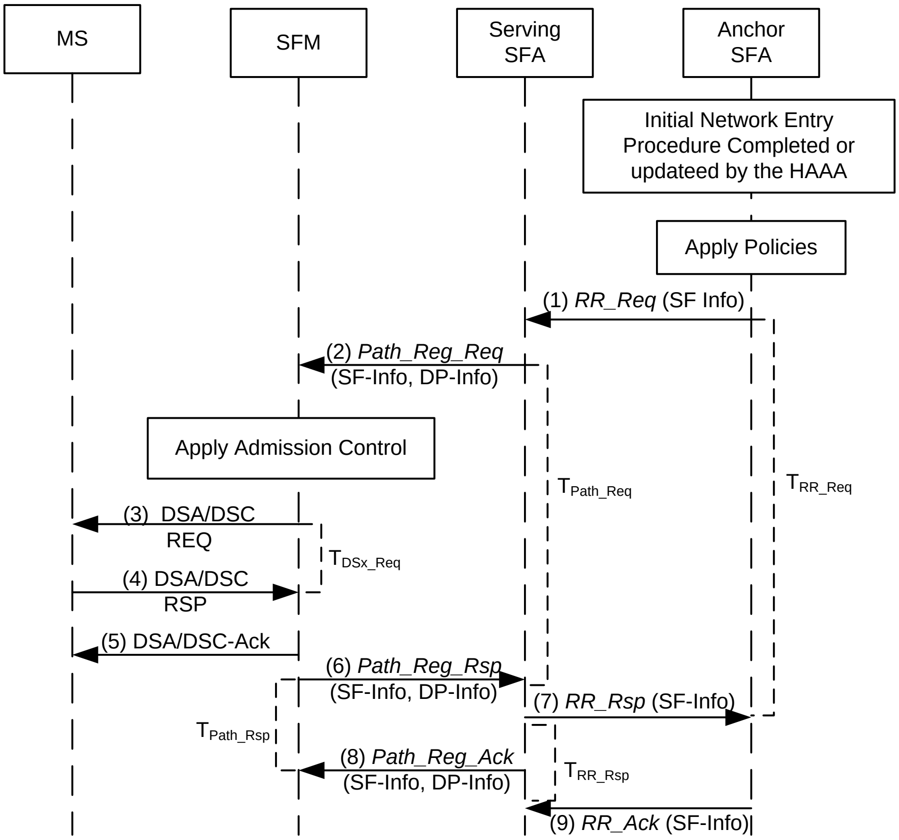


Figure 4-81 – SFA-Triggered Service Flow Creation (Profile Downloaded in SFA)

STEP 1

The initial QoS profile or a modification for it was received at the Anchor-SFA. *RR_Req* according to Table 4-63 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 4-71 (if a new DP is required) or a *Path_Modification_Req* according to Table 4-76 (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 of *Path_Reg_Req*, a DSA-REQ according to IEEE802.16e [11] is sent to the MS/AMS, and in case of acceptance of *Path_Modification_Req* a DSC-REQ according to IEEE802.16e [11] is sent to the MS/AMS.

STEP 4

MS/AMS 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/AMS to complete the QoS transaction.

STEP 6

Assuming acceptance by SFM in step 3 and acceptance by MS/AMS 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 4-73 / Table 4-76 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 4-68 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/AMS 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.

4.6.4.6.3 MS/AMS Initiated Service Flow Creation

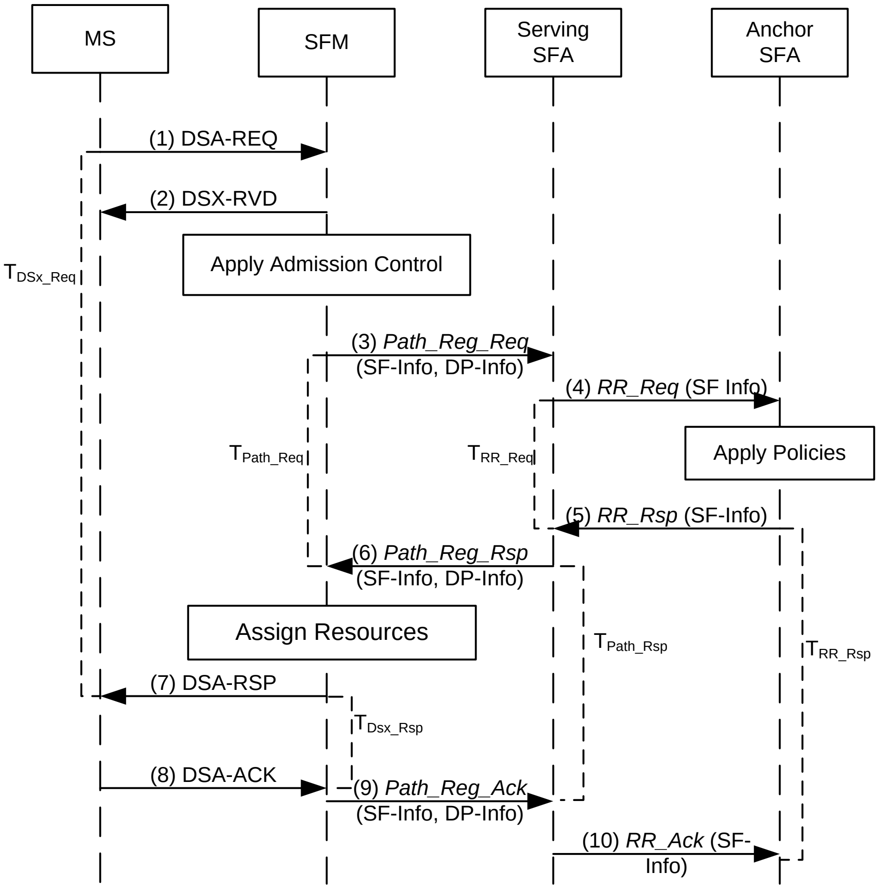


Figure 4-82 – MS/AMS Initiated Service Flow Creation

STEP 1

A DSA-REQ was received by the SFM from the MS/AMS.

STEP 2

According to IEEE802.16e [11] a *DSX-RVD* is sent to the MS/AMS.

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_Registratoin_Req* according to Table 4-72 to the Serving-SFA to trigger DP and SF reservation. The *Path_Registration_Req* include the QoS-Info TLV received from the MS/AMS.

STEP 4

RR_Req according to Table 4-64 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 4-68 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 4-74 to the SFM to confirm the reservation.

STEP 7

The SFM confirMS/AMS the request of the MS/AMS by DSA-RSP message.

STEP 8

MS/AMS sends a DSA-ACK to complete the QoS-request.

STEP 9

SFM sends a *Path_Registration_Ack* according to section Table 4-75 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 4-70 to complete the QoS-request.

4.6.4.6.4 MS/AMS Initiated Service Flow Modification

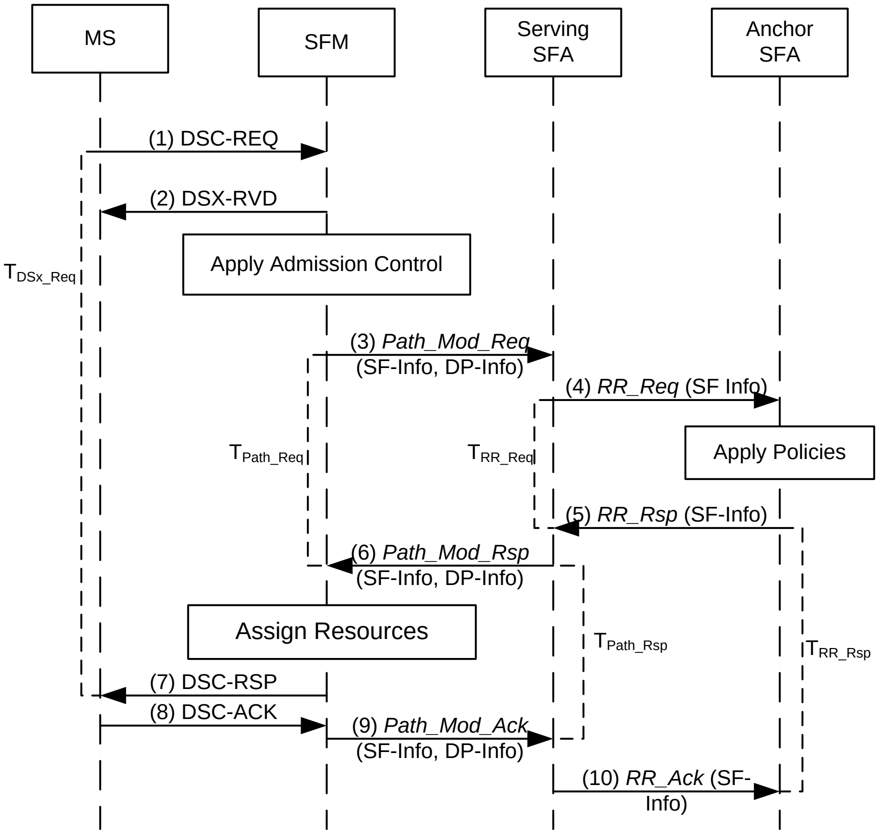


Figure 4-83 – MS/AMS initiated Service Flow Modification

STEP 1

A DSC-REQ was received by the SFM from the MS/AMS.

STEP 2

According to IEEE802.16e [11] a *DSX-RVD* is sent to the MS/AMS.

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 4-76 to the Serving-SFA. The *Path_Modification_Req* include the QoS-Info TLV received from the MS/AMS.

STEP 4

RR_Req according to Table 4-63 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 4-68 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 4-76 to the SFM to confirm the reservation.

STEP 7

The SFM confirMS/AMS the request of the MS/AMS by DSC-RSP message.

STEP 8

MS/AMS sends a DSC-ACK to complete the QoS-request.

STEP 9

SFM sends a *Path_Modification_Ack* according to section Table 4-78 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 4-70 to complete the QoS-request.

4.6.4.6.5 Network Initiated Service Flow Deletion

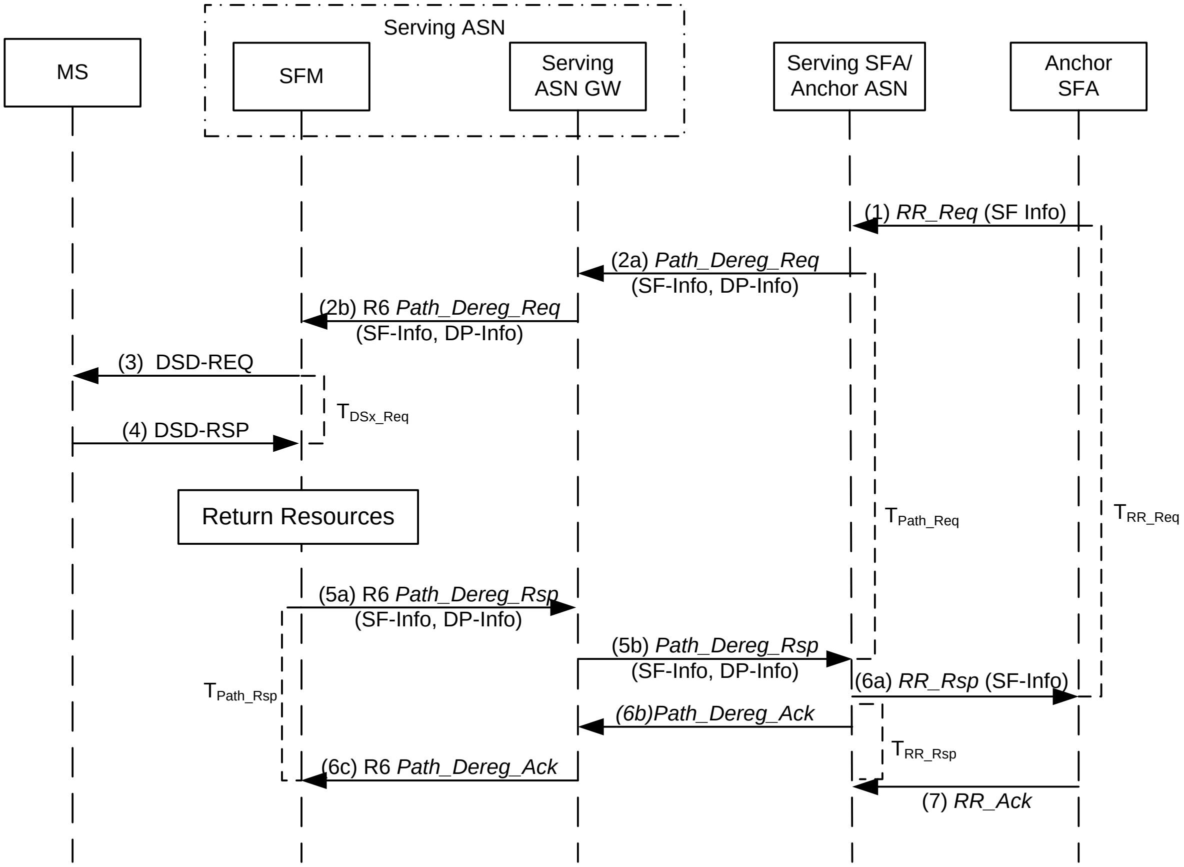


Figure 4-84 – SFA-Triggered Service Flow Deletion

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 4-67 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/ABS).

STEP 3

The SFM send a DSD-REQ according to IEEE802.16e [11] to the MS/AMS.

STEP 4

The MS/AMS sends a DSD-RSP according to IEEE802.16e [11] back to the SFM.

STEP 5

Upon receiving the response from the MS/AMS, the SFM sends *Path_Dereg_Rsp* message according to Table 4-80 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 4-69 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 4-70 SHALL be sent to the Serving-SFA as acknowledgement.

4.6.4.6.6 MS/AMS Initiated Service Flow Deletion

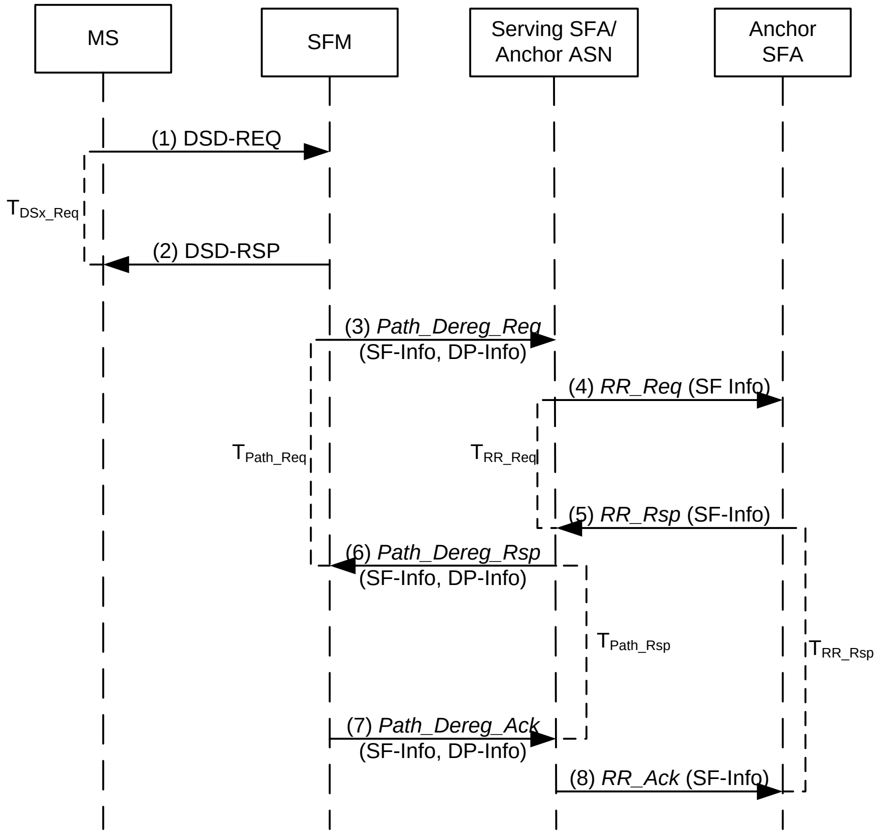


Figure 4-85 – MS/AMS-Triggered Service Flow Deletion

STEP 1

The SFM receives DSD-REQ from MS/AMS.

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 4-70 to the Anchor-SFA as an acknowledgement. The Anchor-SFA SHALL then also release the context.

4.6.4.6.7 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 4-60):

- 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 4-60 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 4-60 – 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 1)
T_{Path_Rsp}			TBD
T_{RR_Rsp}			TBD
T_{Dsx_Rsp}			300msec2)

1) According to T_7 of IEEE802.16e.

2) According to T_8 of IEEE802.16e.

4.6.4.6.8 SF Management Error Conditions

This section describes error conditions associated with the SF management procedure.

4.6.4.6.8.1 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 4-61.

Table 4-61 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
T_{RR_Req}	Anchor SFA	The Authenticator ASN SHALL initiate network exit procedure and send an Accounting Start message (if not already sent) followed by an Accounting Stop message including an error cause.
T_{RR_Req}	Serving SFA	The Serving SFA SHALL initiate network exit procedure.
T_{Path_Req}	Serving SFA	Sends *RR_Rsp* message with Failure Indication TLV set to “Timer expired without response”.
T_{Path_Req}	SFM	In the case of service flow addition or modification, the SFM SHALL send DSA/DSC-RSP with appropriate failure indication to the MS/AMS.
T_{DSx_Req}	SFM	Sends *Path_Dereg_Rsp* and *Path_Modification_Rsp* with Failure Indication TLV set to “Timer expired without response”. In the case of SF deletion the SFM SHALL release the associated resources.
T_{Path_Rsp}	SFM	The requested or deleted resources should be released. The deletion of the SFs on the MS/AMS should be triggered as described in Figure 4-84 step 3 and 4.
T_{Path_Rsp}	Serving SFA	The Serving SFA SHALL continue to assign the requested resources and release the resources that are deleted.
T_{RR_Rsp}	Serving SFA	The requested or deleted resources should be released. The deletion of the SFs on the MS/AMS should be triggered as described in Figure 4-84 step 2 to 5.
T_{Dsx_Rsp}	SFM	Sends *Path_Reg_Ack* and *Path_Modification_Ack* with Failure Indication TLV set to “Timer expired without response”.

4.6.4.6.8.2 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/AMS (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.

4.6.4.6.8.3 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/AMS.

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/AMS 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 4-62 – Data Path Control Messages

QoS Control Message	Data Path Control Message
RR_Req / RR_Rsp/ RR_Ack (Create)	*Path_Reg_Req*, *Path_Reg_Rsp* and *Path_Reg_Ack*, or *Path_Modification_Req, Path_Modification_Rsp*, and *Path_Modification_Ack* if new SF uses existing DP.
RR_Req / RR_Rsp/ RR_Ack (Modification)	*Path_Modification_Req, Path_Modification_Rsp*, and *Path_Modification_Ack.*
RR_Req / RR_Rsp/ RR_Ack (Delete)	*Path_Dereg_Req, Path_Dereg_Rsp* and *Path_Dereg_Ack*, or *Path_Modification_Req, Path_Modification_Rsp*, and *Path_Modification_Ack* if DP is shared by another SF.

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 4-63 – 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/AMS. The flag can be applied on a per MS/AMS 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/AMS and the level of the indication (i.e., per MS/AMS 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".
>>SFID	5.3.2.184	M	SFID as defined on R1.

IE	Reference	M/O	Notes
>>SF Type	5.3.2.306	O	
>>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/AMS'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.
>>>IPv6 Flow Label	5.3.2.470	O	
>>QoS Parameters	5.3.2.141	M	
>>> DSCP	5.3.2.409	O	TC bit is set to 1

IE	Reference	M/O	Notes
>>>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 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.

IE	Reference	M/O	Notes
>>>>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).
>>>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	0	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.
>>SF Operation Policy	5.3.2.459	O	This TLV is to specify the SF operation policy for a given service flow. If the ASN has indicated the support of the per SF airlink encryption on/off capability, the “absence” of this TLV implies the airlink encryption decision is a local implementation policy at the ASN. (NOTE: This indication applies to SF creation phase but not for the SF modification phase)
>>Local Routing Policy	5.3.2.538	O	This TLV is to specify the Local Routing policy for a given service flow.
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

4.6.5.2.2 Service Flow Creation (Serving-SFA to Anchor-SFA)

Table 4-64 – 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/AMS. The flag can be applied on a per MS/AMS 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/AMS and the level of the indication (i.e. per MS/AMS 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	
>>SF Type	5.3.2.306	O	
>>Reservation Action	5.3.2.151	M	SHALL be set to "Create, Admit and Activate".
>>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.

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.
>>>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.
>>>IPv6 Flow Label	5.3.2.470	O	
>>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

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.
>>>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	0	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 (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 4-65 – 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 or Activate”.
>>SFID	5.3.2.184	M	SFID as defined on R1.

Following definition show the message where any parameter could be modified.

Table 4-66 – RR_Req: SF Modification, parameter modification only (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/AMS. The flag can be applied on a per MS/AMS 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/AMS and the level of the indication (i.e. per MS/AMS 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.
>>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.

IE	Reference	M/O	Notes
>>>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.
>>>IPv6 Flow Label	5.3.2.470	O	
>>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

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.
>>>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	0	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 4-67 – 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 or Modification

Table 4-68 – RR_Rsp: SF Creation or Modification

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.
>>SF Type	5.3.2.306	O	
>>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 hast 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 *RR_Req* 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.

IE	Reference	M/O	Notes
>>>>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 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.
>>Local Routing Policy	5.3.2.538	O	This TLV is to specify the Local Routing policy for a given service flow.

4.6.5.3.2 Service Flow Deletion

Table 4-69 – RR_Rsp: Deletion of a SF

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>SF Info	5.3.2.185	M	
>>SFID	5.3.2.184	M	SFID as defined on R1.
>>Reservation Result	5.3.2.152	M	

4.6.5.3.3 RR_Ack

Table 4-70 – 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. The SFM initiates the Path-Reg_Req in the opposite direction in the case of MS/AMS initiated SF creation or modification. 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 5.3.2.

Table 4-71 – 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/AMS. The flag can be applied on a per MS/AMS 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/AMS and the level of the indication (i.e., per MS/AMS level or per CS

IE	Reference	M/O	Notes
			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.
>>SF Type	5.3.2.306	O	
>>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. One or more classification rules per service flow can be provided in a single message.
>>>Classification Rule Index	5.3.2.30	O	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.
>>>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.

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.
>>>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.
>>>IPv6 Flow Label	5.3.2.470	O	
>>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	O	This TLV SHALL be included for Uplink direction 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	5.3.2.95	O	See IEEE802.16e for further details.

IE	Reference	M/O	Notes
Traffic Rate			
>>>>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	O	This TLV SHALL be included for Uplink direction 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.
>>>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	O	This TLV SHALL be included for Uplink direction 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	O	
>>>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	One or more PHS rules per service flow can be provided in a single message.
>>>PHSI	5.3.2.125	O	This TLV SHALL be included if PHS Rule is included in the transmitted message.
>>>PHSS	5.3.2.129	O	This TLV may not be included at the time of service flow creation.
>>>PHSF	0	O	This TLV may not be included at the time of service flow creation.
>>>PHSM	5.3.2.126	O	This TLV may not be included at the time of service flow creation.

IE	Reference	M/O	Notes
>>>PHSV	5.3.2.130	O	This TLV may not be included at the time of service flow creation.
>>SF Operation Policy	5.3.2.459	O	This TLV is to specify the SF operation policy for a given service flow. If the ASN has indicated the support of the per SF airlink encryption on/off capability, the “absence” of this TLV implies the airlink encryption is a local implementation policy at the ASN. (NOTE: This indication applies to SF creation phase but not for the SF modification phase)
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

1

2 Table 4-72 – Path-Reg-Req: Creation of SF and DP (MS/AMS 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/AMS. The flag can be applied on a per MS/AMS 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/AMS and the level of the indication (i.e. per MS/AMS 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	Due to no SF IDs, service flows are restricted to one uplink and one downlink flow.
>>SFID	5.3.2.184	O	SFID is assigned by the ASN-GW and not the MS/AMS and therefore is not included in this message. It is left in this message as optional to support legacy 1.0 equipment which may still send it. Note: If R1.0 is updated via a CR, , this TLV should be removed from this message.
>>SF Type	5.3.2.306	O	
>>Reservation Action	5.3.2.151	M	MUST be set to “Create, Admit and Activate”

IE	Reference	M/O	Notes
>>Direction	5.3.2.59	M	Specifies the direction of the reservation.
>>CID	5.3.2.29	O	This identifier is only mandatory if a DataPath of Type 2 is used between SFA and SFM. 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. Multiple classification rules per service flow can be present in the message only if no PHS rules are provided at the same time for this service flow. If both a Classification Rule and a PHS Rule are provided for a service flow, only one instance of each will be included due to R1 limitations.
>>>Classification Rule Index	5.3.2.30	O	MS/AMS may not assign a PCRI value and therefore, the TLV may not be included.
>>>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.

IE	Reference	M/O	Notes
>>>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.
>>>IPv6 Flow Label	5.3.2.470	O	
>>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
>>>>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	O	This TLV SHALL be included for Uplink direction 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.

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.
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction 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	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.
>>>>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	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	O	Identifies the Data Path which SHALL be used for the service flow. MS/AMS includes the data path information for DL flows only.
>>>Data Path ID	5.3.2.44	O	This TLV SHALL be included if the parent TLV is included in the message.
>>>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	

IE	Reference	M/O	Notes
>>>PHS Rule	5.3.2.127	O	Not more than one PHS rule per service flow in a single message is allowed due to R1 limitations.
>>>PHSI	5.3.2.125	O	This TLV may not be included at the time of service flow creation.
>>>PHSS	5.3.2.125	O	This TLV may not be included at the time of service flow creation.
>>>PHSF	0	O	This TLV may not be included at the time of service flow creation.
>>>PHSM	5.3.2.126	O	This TLV may not be included at the time of service flow creation.
>>>PHSV	5.3.2.130	O	This TLV may not be included at the time of service flow creation.
>BS Info	5.3.2.26	O	
>>BS ID	5.3.2.25	CM	

Table 4-73 – 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	
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 *RR_Req* 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	5.3.2.150	CM	See IEEE802.16e for further details.

IE	Reference	M/O	Notes
Policy			
>>>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	O	This TLV SHALL be included for Uplink direction 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	O	This TLV SHALL be included for Uplink direction 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	O	This TLV SHALL be included for Uplink direction 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).
>>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	O	Data Path Identifier (e.g., GRE key). Mandatory if DP Info TLV is included. Will be included for the receive side of the entity sending the message.
>>>Tunnel Endpoint	5.3.2.194	O	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

1 **Table 4-74 – Path-Reg-Rsp: Creation of SF and DP (MS/AMS 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.
>>SF Type	5.3.2.306	O	
>>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.
>>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 hast to be present in response messages sent from Serving-SFA to BS/ABS as far as a classifier was present in the request.
>>>Classification Rule Index	5.3.2.30	O	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/ABS.
>>>Classification Rule Priority	5.3.2.32	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>Protocol	5.3.2.138	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>IP Source Address and Mask	5.3.2.84	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>IP Destination Address and Mask	5.3.2.82	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>Protocol Source Port Range	5.3.2.140	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>Protocol Destination Port Range	5.3.2.139	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>ROHC Parameter	7.3.2.1 of [8]	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>Associated PHSI	5.3.2.15	O	TLV shall be included if a PHS rule was defined by MS/AMS for this classifier.
>>>MAC Source Address and Mask	5.3.2.384	O	TLV shall be included if sent by MS/AMS and parent TLV is present.

IE	Reference	M/O	Notes
>>>MAC Destination Address and Mask	5.3.2.385	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>ETYPE/SAP	5.3.2.386	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>User Priority Range	5.3.2.387	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>SVLAN ID	5.3.2.393	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>CVLAN ID	5.3.2.394	O	TLV shall be included if sent by MS/AMS and parent TLV is present.
>>>IPv6 Flow Label	5.3.2.470	O	
>>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 *RR_Req* 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	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	O	This TLV SHALL be included for Uplink direction 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.

IE	Reference	M/O	Notes
>>>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	O	This TLV SHALL be included for Uplink direction 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	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	O	This TLV SHALL be included for Uplink direction 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.

IE	Reference	M/O	Notes
>>>>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	
>>PHS Rule	5.3.2.127	O	TLV shall be included if provided by the MS/AMS.
>>>PHSI	5.3.2.125	O	TLV shall be included if parent TLV is present.
>>>PHSS	5.3.2.125	O	TLV shall be included if parent TLV is present and TLV was provided by MS/AMS.
>>>PHSF	0	O	TLV shall be included if parent TLV is present and TLV was provided by MS/AMS.
>>>PHSM	5.3.2.126	O	TLV shall be included if parent TLV is present and TLV was provided by MS/AMS.
>>>PHSV	5.3.2.130	O	TLV shall be included if parent TLV is present and TLV was provided by MS/AMS.
>>Tunnel Endpoint	5.3.2.194	O	
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	

Table 4-75 – 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	
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS/ABS 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. The SFM initiates the Path-Reg_Req in the opposite direction in the case of MS/AMS initiated SF creation or modification. 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 4-76 – 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/AMS. The flag can be applied on a per MS/AMS 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/AMS and the level of the indication (i.e., per MS/AMS 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. Not more than one classification rule per service flow is allowed in a single Path_Mod_Req message due to R1 limitations.
>>>Classification Rule Index	5.3.2.30	O	For Network initiated flows, this TLV SHALL be included if Packet Classification Rule/ Media Flow Description is included in the transmitted message. For MS/AMS initiated flows, the TLV is Optional – since MS/AMS is not responsible for assigning PCRI, this TLV may not be in the 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.
>>>IPv6 Flow Label	5.3.2.470	O	

IE	Reference	M/O	Notes
>>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.
>>>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	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.
>>>>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.
>>>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.
>>>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	O	This TLV SHALL be included for Uplink direction 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.
>>>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	O	This TLV SHALL be included for Uplink direction 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.
>>>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 may be Present only for the Service Flow which the Sender is responsible for creating.
>>>Data Path ID	5.3.2.44	O	This TLV SHALL be present if the Parent TLV is included in the message.
>>> Data Path Type	5.3.2.46	O	
>>>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 the SDU Info is included in the transmitted message.

IE	Reference	M/O	Notes
>>>SDU BSN Map	5.3.2.175	O	
>>PHS Rule	5.3.2.127	O	Not more than one PHS rule per service flow is allowed in a single Path_Mod_Req message due to R1 limitations.
>>>PHSI	5.3.2.125	O	This TLV SHALL be included if PHS Rule is included in the transmitted message. Since MS/AMS is not responsible for assigning PHSI, for MS/AMS initiated flows this TLV may not be in the message.
>>>PHSS	5.3.2.129	O	This TLV SHALL be included if PHS Rule is included in the transmitted message. The TLV shall be included if sent by MS/AMS.
>>>PHSF	0	O	This TLV SHALL be included if PHS Rule is included in the transmitted message. The TLV shall be included if sent by MS/AMS.
>>>PHSM	5.3.2.126	O	This TLV SHALL be included if PHS Rule is included in the transmitted message. The TLV shall be included if sent by MS/AMS.
>>>PHSV	5.3.2.130	O	This TLV SHALL be included if PHS Rule is included in the transmitted message. The TLV shall be included if sent by MS/AMS.
>>>PHS Rule Action	5.3.2.128	O	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 4-77 – 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	

IE	Reference	M/O	Notes
>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	In the case of network-initiated service flows, this is only allowed to be present if "Reduced Resources Code" was set at the corresponding *RR_Req* message.
>>Packet Classification Rule/ Media Flow Description	5.3.2.114	O	For MS/AMS-initiated service flow modification, this TLV will be included if provided by MS/AMS in the request message and modification is authorized.
>>>Classification Rule Index	5.3.2.30	O	The TLV shall be included if parent TLV is present.
>>>Classification Rule Action	5.3.2.31	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>Classification Rule Priority	5.3.2.32	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>Protocol	5.3.2.138	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>IP Source Address and Mask	5.3.2.84	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>IP Destination Address and Mask	5.3.2.82	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>Protocol Source Port Range	5.3.2.140	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>Protocol Destination Port Range	5.3.2.139	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.

IE	Reference	M/O	Notes
>>>Associated PHSI	5.3.2.15	O	For MS/AMS-initiated service flow modification, the TLV shall be included if a PHS rule needs to be associated with the classifier.
>>>MAC Source Address and Mask	5.3.2.384	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>MAC Destination Address and Mask	5.3.2.385	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>ETYPE/SAP	5.3.2.386	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>User Priority Range	5.3.2.387	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>SVLAN ID	5.3.2.393	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>CVLAN ID	5.3.2.394	O	For MS/AMS-initiated service flow modification, the TLV shall be included if provided by MS/AMS.
>>>IPv6 Flow Label	5.3.2.470	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.
>>>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	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.
>>>>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.
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.

IE	Reference	M/O	Notes
>>>>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.
>>>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	O	This TLV SHALL be included for Uplink direction 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.
>>>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	O	This TLV SHALL be included for Uplink direction 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.
>>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.

IE	Reference	M/O	Notes
>>>Data Path ID	5.3.2.44	O	Data Path Identifier (e.g., GRE key). Mandatory if DP Info TLV is included. Will be included for the receive side of the entity sending the message.
>>>Tunnel Endpoint	5.3.2.194	O	
>>PHS Rule	5.3.2.127	O	For MS/AMS-initiated SF modification, the TLV SHALL be included if provided by MS/AMS in the request message and modification is authorized.
>>>PHSI	5.3.2.125	O	For MS/AMS-initiated SF modification, the TLV SHALL be included if provided by MS/AMS in the request message.
>>>PHSS	5.3.2.125	O	For MS/AMS-initiated SF modification, the TLV SHALL be included if provided by MS/AMS in the request message.
>>>PHSF	0	O	For MS/AMS-initiated SF modification, the TLV SHALL be included if provided by MS/AMS in the request message.
>>>PHSM	5.3.2.126	O	For MS/AMS-initiated SF modification, the TLV SHALL be included if provided by MS/AMS in the request message.
>>>PHSV	5.3.2.130	O	For MS/AMS-initiated SF modification, the TLV SHALL be included if provided by MS/AMS in the request message.
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 4-78 – 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/ABS 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 4-79 – Path_Dereg_Req: Deletion of SF and/or DP / MS/AMS Network Exit Procedure

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	O	
>Anchor ASN GW ID	5.3.2.10	O	Unique Identifier of the Anchor GW (Anchor DP entity). Present when the ASNGW function is not co-located at serving GW.
>Authenticator ID	5.3.2.19	O	Unique Identifier of the Anchor Authenticator entity. Present when the authenticator function is not co-located at serving GW.
>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. If absent then it implies all actives service flows are de-registered. (e.g., both normal data path and BS Buffer Switching data path are de-registered if the data paths had been established in BS buffer switching method.)
>>Reservation Action	5.3.2.151	O	SHALL be set to “Delete”.
>>SFID	5.3.2.184	O	SFID as defined on R1.
>>Data Path Info	5.3.2.45	O	
>>>Data Path ID	5.3.2.44	O	If Data Path Info is present, then at least one of Data Path ID or Switching Data Path ID shall be present.
>>>Switching Data Path ID	5.3.2.383	O	If Data Path Info is present, then at least one of Data Path ID or Switching Data Path ID shall be present.
>>CID	5.3.2.29	O	This identifier is only mandatory if a DataPath of Type 2 is used between SFA and SFM.
Action Code	5.3.2.3	O	Included only when the message is directed to a Serving BS/ABS and if it carries the instruction for MS/AMS Network Exit. Deregistration instruction for the MS/AMS.
Network Exit Indicator	5.3.2.109	O	Included only when the message is sent from DPF

IE	Reference	M/O	Notes
			in Serving BS/ABS to Relay DPF and from Relay DPF to Anchor DPF. If present, indicates the reason of MS/AMS Network Exit (e.g., MS/AMS Power Down indication, radio link with MS/AMS is lost, etc.).
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 4-80 – 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	O	Unique Identifier of the Anchor GW (Anchor DP entity). Present when the ASNGW function is not co-located at serving GW.
>SF Info	5.3.2.185	O	Absence indicates all active flows must be deleted.
>>SFID	5.3.2.184	O	SFID as defined on R1.
>>Reservation Result	5.3.2.152	O	
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	

Table 4-81 – Path_Dereg_Ack: Deletion of Service Flow and DP

IE	Reference	M/O	Notes
BS Info	5.3.2.26	O	
>BS ID	5.3.2.25	CM	
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/AMS.

Thus the Anchor/Serving SFA SHALL keep track of the SFIDs that have been already assigned to the MS/AMS. This is possible because the SFA is by definition the entity that takes care of service authorization for each particular MS/AMS. Thus the Anchor/Serving SFA simply assigns a new SFID by selecting a value, which is not yet in use in the MS/AMS 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/m DSx message exchange with the MS/AMS. The particular SFID of “0x0001” is reserved for DSF at the SFA/SFM and the AMS, and need not be sent by the Anchor SFA in the Path_Registration_Request messages to initiate the Service Flow creation. The SFM shall not trigger the IEEE 802.16e/ DSx message exchange for the DSF.

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/AMS

MS/AMS 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/AMS as well as in the network side.

AMS SHALL be provisioned with the QoS parameters information for Default Service Flow which is necessary for the initial network entry at the MZone of an ABS, regardless of the presence of the QoS profile. The information includes SFID, FID, scheduling type, maximum bandwidth allowed/sustained, traffic priority, packet classification rules, etc.

Per operator policy, QoS profile MAY be configured in the MS/AMS whenever QoS Profile of the subscriber is created or changes. It is implementation specific how the MS/AMS 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/AMS:

- TotalTrafficRate: Maximum value of sum of Maximum Sustained Traffic Rate parameters of existing SFs created by MS/AMS. This parameter is optional.
- Service Flow (zero or more)
    - Number of SFs: Number of this kind of SFs that the MS/AMS 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/AMS 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/AMS is allowed to use per this SF profile. This parameter is optional.
    - Maximum Latency: Minimum value of maximum latency that the MS/AMS 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/ABSs and one or more ASN GWs. The BSs/ABSs 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/ABSs that hosts Serving HO Function and serves the MS/AMS prior to HO.

b. Target BS/ABSs that hosts Target HO Function. There might be one or more Target BSs/ABSs. One of them is selected as the final HO Target and becomes Serving BS/ABSs after HO completion.

c. Relay ASN GW that relays the HO Control messages between the Serving and Target BSs/ABSs 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/ABSs (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/ABSs. The Target ASN GW MAY be located on the path between the Anchor ASN GW and the Target BS/ABSs. 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[7]

Upon reception of a MOB-MSHO-REQ message from a mobile station (MS) or a AAI-HO-REQ message from an advanced mobile station (AMS), the Serving BS/ABS SHALL initiate a handover to one or more candidate Target BSs/ABSs by sending a *HO_Req* message to each Target BS/ABSs over the R6 interface. If a Target BS/ABS is connected to another ASN-GW, the *HO_Req* message is relayed over R4 to the Target BS/ABS. The Relay ASN-GW SHALL relay the message(s) to the Target BS(s) /ABS(s) over the R6/R4 interface(s). If no acceptable Target BS/ABS is available, the Serving BS/ABS sends a MOB_BSHO-RSP/AAI-HO-CMD message to the MS/AMS containing no potential Target BS/ABS to reject the handover. If the MS mobility access classifier is fixed or nomadic and the BS/ABS supports mobility restriction for stationary access, only Target BSs/ABSs that belong to the MS Reattachment zone may be selected for a handover.

If the MS/AMS sends a MOB_MSHO-REQ/AAI-HO-REQ to the Serving BS/ABS without including any preferred Target BSs/ABSs, the Serving BS/ABS MAY respond with a MOB_BSHO-RSP message with the Mode field set to ‘0b111’ or with a AAI-HO-CMD message with the Mode field set to ‘0b10’ (MS/AMS handover request not recommended [BS/ABS in list unavailable]), or the Serving BS/ABS MAY select and recommend a Target BS(s)/ABS(s) to the MS/AMS in the MOB_BSHO-RSP/AAI-HO-CMD message.

[7] This section describes handover control procedures which are applicable to handovers occurring between two Legacy BSs or between two Advanced BSs. For the handover control procedures between a Legacy BS and an Advanced BS, refer to subsection 4.7.4.

The Serving BS/ABS SHALL silently discard duplicate MOB_MSHO-REQ/AAI-HO-REQ messages from an MS/AMS if it has already initiated the HO preparation phase for the MS/AMS. If a Serving BS/ABS receives a duplicate MOB_MSHO-REQ/AAI-HO-REQ from an MS/AMS, it SHALL not propagate the request further into the network.

A Relay ASN-GW involved in the handover has no handover related intelligence, therefore the Serving BS/ABS SHALL be required to send a separate R6 *HO_Req* message for each potential Target BS/ABS.

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/ABS(s) MAY retrieve AK context from the Authenticator ASN-GW. The Target BS/ABS(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 4-86.

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/AMS' Authenticator SHALL reject AK context requests for/from the unauthorized Target BS/ABSs based on Authenticator's knowledge of MS Reattachment Zone list. To reject the AK context request for/from the Target BS/ABS, the MS/AMS' Authenticator responds with Context-Rpt message that includes appropriate Failure Indication value and excludes MS/AMS' AK context.

The Serving BS/ABS may have no knowledge with respect to whether authenticator or data path functions are co-located at the Serving ASN-GW. The Serving BS/ABS 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/ABS to Target BS/ABS for 802.16e mode handovers 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/ABS (s) MAY pre-establish the data path for the MS/AMS with the Anchor ASN-GW. If the Target BS/ABS (s) decides to pre-establish the data path, the Target BS/ABS 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 4-86.

Data Path Pre-Registration at the Handover Preparation Phase is optional and may be executed only when both Target BS/ABS and Anchor ASN-GW support this functionality. If the Anchor ASN-GW does not support Data Path Pre-Registration and the Target BS/ABS 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/ABS).

The Target BS/ABS SHALL respond to the *HO_Req* message with the *HO_Rsp* message, and the Serving BS/ABS SHALL acknowledge the Handover Preparation transaction completion by sending a *HO_Ack* message (see Figure 4-86 and Figure 4-87 for the call flow scenarios).

In the case Target BS/ABS tries and fails to acquire MS security context (AK context) in the HO Preparation Phase, it SHALL respond with the *HO_Rsp* message including either the appropriate BS/ABS HO RSP Code value or Failure Indication.

The Serving/Anchor and Target ASN-GWs, MAY optionally include the relevant Data Path Info TLVs within the relevant HO Control messages. In other words the *HO_Req* message may also include the data path control information contained in the *Path_Prereg_Req* message and the *HO_Rsp* message may include the information contained in the *Path_Prereg_Rsp* message. The *HO_Ack* message will also serve as the *Path_Prereg_Ack* message.

The combining or piggybacking of data path pre-registration messages over handover control messages is possible only when both Anchor ASN-GW and Target BS/ABSs support this feature. The Anchor ASN-GW MAY initiate this procedure, but if the Target BS/ABS doesn't support message combining it will simply ignore the Data Path Info TLVs in the *HO_Req* message and respond with a *HO_Rsp* message which doesn't contain any Data Path Info TLVs. In this case the Target BS/ABS MAY initiate Data Path Pre-Registration on its own (i.e., proceed according to the Scenario 2, shown in Figure 4-87).

If the Target BS/ABS supports HO Control and Data Path Control message combining and receives a *HO_Req* message combined with *Data Path Info* TLVs, it SHALL respond with the *HO_Rsp* message combined with *Data Path Info* TLVs. Consequently, a *HO_Ack* message SHALL be sent by the Serving BS/ABS as the acknowledgment of the *HO_Rsp* message.

Target BS/ABS MAY initiate Data Path Pre-Registration procedure on its own.

Upon successful 3-way Data Path Pre-registration procedure, Target BS/ABS SHALL start the Path Retain timer. The Path Retain timer is used to delete pre-registered Data Path in the event the MS does not handover to the Target BS/ABS and Data Path Deregistration is not received from the Anchor ASN-GW.

To summarize, data path pre-registration during the handover preparation phase is optional and may occur when both the Target BS/ABS and the Anchor ASN-GW support the procedure. The Target BS/ABS or the Anchor ASN-GW may choose not to perform data path pre-registration. Retrieval of AK Context from the Authenticator by the Target ASN-GW during the Handover Preparation phase is also optional and may otherwise occur during the Handover Action phase.

4.7.2.1.1 Handover Preparation Scenario 1: AK Context Retrieval and Path Pre-Registration Initiated by Target BS/ABS

The following call flow describes a successful inter-ASN handover preparation scenario where the Serving BS/ABS provides the Target BS/ABS with the Authenticator ID and the Target BS/ABS pre-establishes the data path during the preparation phase.

In the HO Preparation Phase, if Anchor ASN-GW is not collocated with the Serving ASN-GW, the *HO_Req* message will not go through Anchor ASN-GW and no data path pre-establishment info can be sent with *HO_Req* to the ASN-GW in the Target ASN. So the data path establishment procedure will be initiated by Target BS/ABS separately.

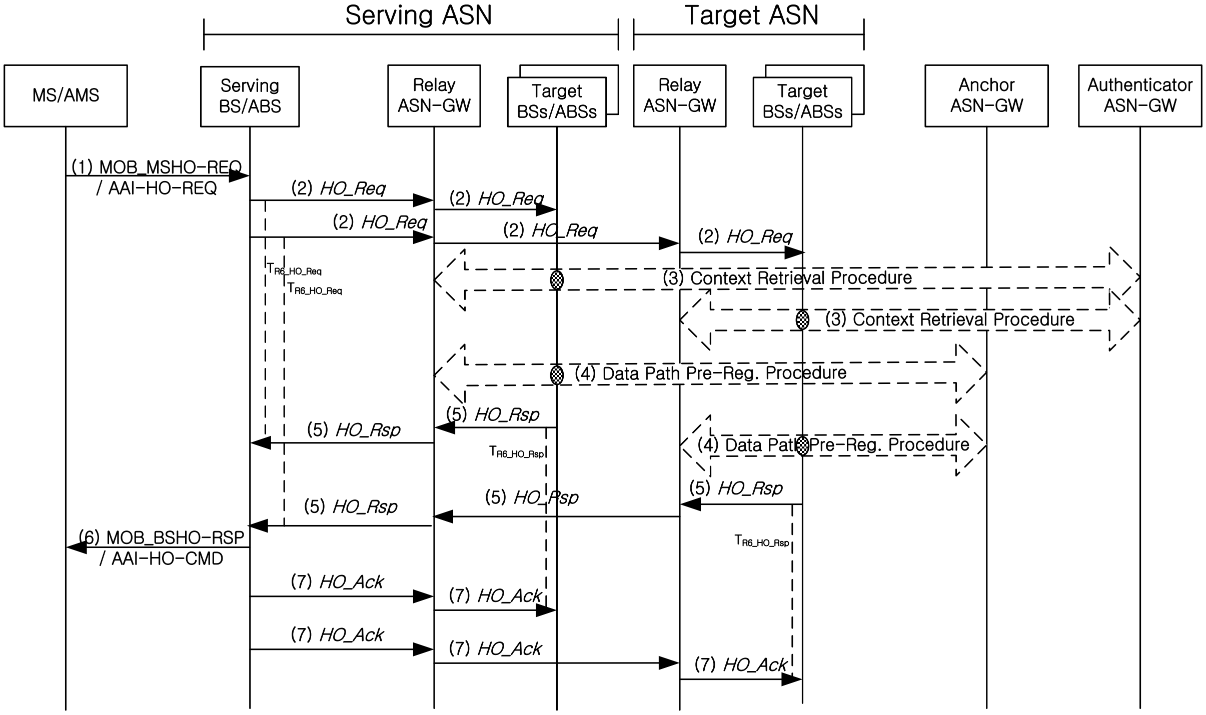


Figure 4-86 – Successful HO Preparation Phase, Scenario 1[8]

STEP 1

The MS/AMS initiates a handover by sending a MOB_MSHO-REQ/AAI-HO-REQ message to the Serving BS/ABS which includes one or more potential Target BS/ABS's.

STEP 2

A Serving BS/ABS SHALL silently discard a duplicate MOB_MSHO-REQ/AAI-HO-REQ from an MS/AMS, if it has already initiated a HO preparation phase for this MS/AMS which is still ongoing. If a Serving BS/ABS receives such duplicate MOB_MSHO-REQ/AAI-HO-REQ from an MS, it SHALL not propagate the request further into the network.

The Serving BS/ABS sends a *HO_Req* message for each Target BS/ABS 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/ABS.

[8] The small grey circle-shaped symbols in the figure denotes that the entities associated with them are one of the end points in the message transactions (represented by block arrows). This convention is used consistently throughout the section.

STEP 3

The Target BS/ABS (s) requests AK context for the MS/AMS by initiating a Context Retrieval 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/ABS initiates a Context Retrieval procedure with the Serving ASN-GW. Note: The Target BS/ABS (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/ABS (s) may initiate pre-establishment of a data path for the MS/AMS 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/ABS (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/ABS (s) may optionally choose to defer this procedure to the handover action phase.

STEP 5

The Target BS/ABS(s) sends a *HO_Rsp* message to the Serving BS/ABS 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/ABS. Upon receipt of the *HO_Rsp* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Req}$.

In the case Target BS/ABS 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/ABS HO RSP Code value or Failure Indication

STEP 6

The Serving BS/ABS sends a MOB_BSHO-RSP/AAI-HO-CMD message to the MS/AMS containing one or more potential Target BS/ABS's selected by the network for the MS/AMS to handover to.[9]

STEP 7

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS (s) controlling the potential Target BS/ABS (s) selected for the MS/AMS. Relay ASN-GW relays the message to the Target BS/ABS(s). Upon receipt of the *HO_Ack* message, the Target BS/ABS(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/ABS. In the scenario, the Target BS/ABS pre-establishes the data paths during the preparation phase.

[9] 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/AMS 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/ABS scheduling and processing times to process the reception of MOB_HO_IND from the MS/AMS by the Serving BS/ABS.

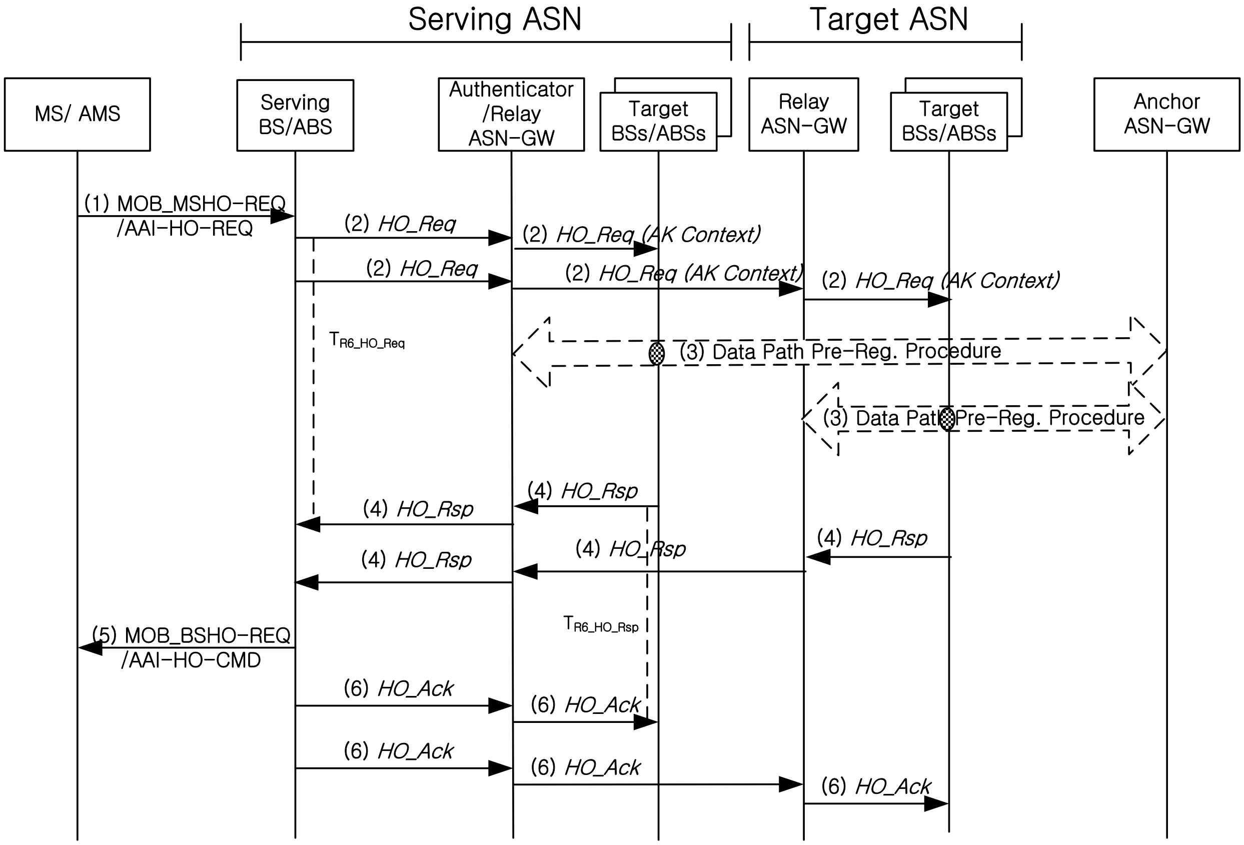


Figure 4-87 – Successful HO Preparation Phase, Scenario 2

STEP 1

The MS/AMS initiates a handover by sending a MOB_MSHO-REQ/AAI-HO-REQ message to the Serving BS which includes one or more potential Target BS/ABS's.

STEP 2

The Serving BS/ABS sends *HO_Req* to one or more Target BS/ABS(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/ABS 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/ABS, the Serving ASN-GW MAY piggyback the AK context for the MS/AMS when sending the *HO_Req* message to the Target BS/ABS. However if AK context is not provided by the MS/AMS' Authenticator for usage with the respective Target BS/ABS, the Serving ASN-GW forwards the *HO_Req* message to this Target BS/ABS 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/ABS pre-establishes a data path for the MS/AMS 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/ABS initiates the Data Path Pre-Registration procedure with the Anchor ASN-GW. Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the handover action phase.

STEP 4

The Target BS/ABS sends a *HO_Rsp* message to the Serving BS/ABS 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/ABS stops timer $T_{R6\_HO\_Req}$.

STEP 5

The Serving BS/ABS sends a MOB_BSHO-RSP/AAI-HO-CMD message to the MS/AMS containing one or more Target BS/ABS's selected by the network for the MS/AMS to handover to[10].

STEP 6

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABSs selected for the MS/AMS via Relay ASN-GW. Upon receipt of the *HO_Ack* message, the Target BS/ABS 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/ABS(s) with the piggybacked handover messages. The handover signaling is optimized by "piggybacking" data path pre-registration signaling onto handover control messages.

[10] Same note as the Note 1

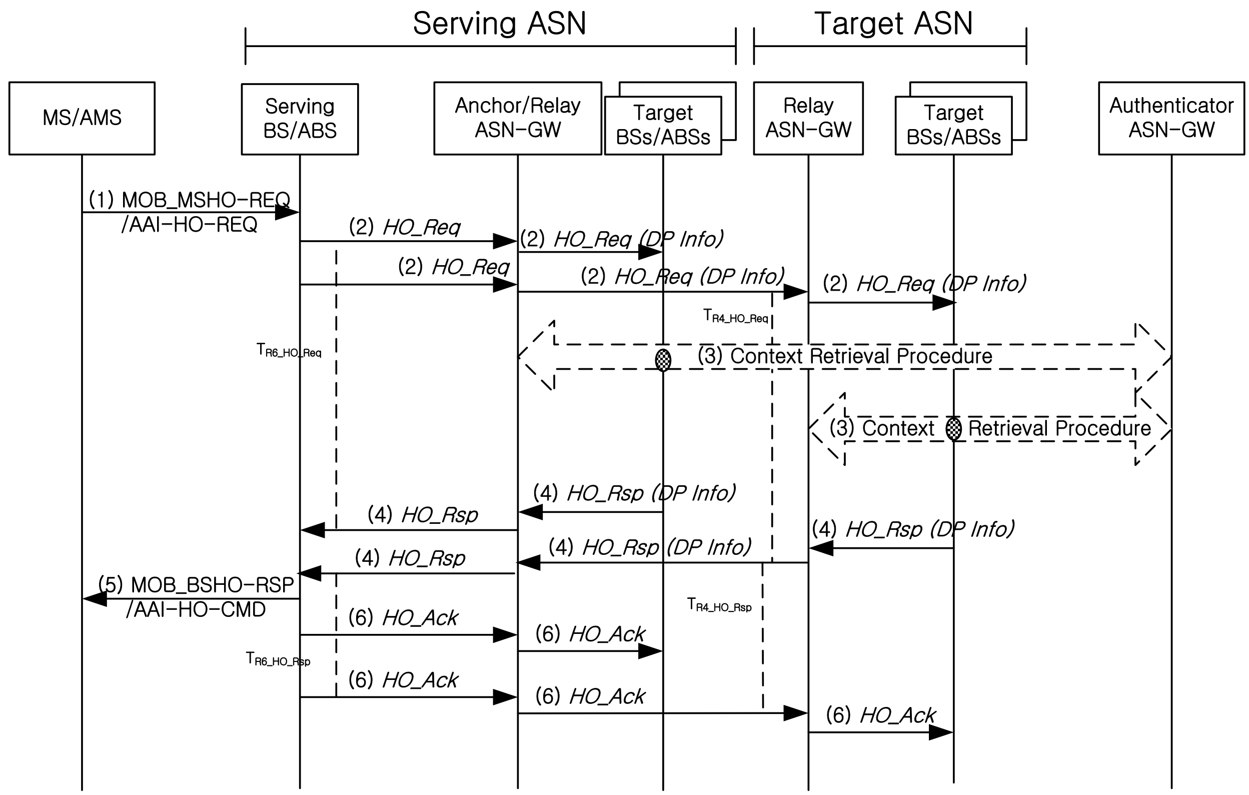


Figure 4-88 – Successful HO Preparation Phase, Scenario 3

STEP 1

The MS/AMS initiates a handover by sending a MOB-MSHO_REQ/AAI-HO-REQ message to the Serving BS/ABS which includes one or more candidate Target BS/ABS'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/ABS, the Serving ASN-GW sends an *HO_Req* message containing the Data Path Info TLV to the Target BS/ABS and starts timer $T_{R4\_HO\_Req}$.

STEP 3

The Target BS/ABS(s) requests AK context for the MS/AMS by initiating a Context Retrieval 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/ABS initiates a Context Retrieval procedure with the Serving ASN-GW. Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the handover action phase.

If AK context request for the particular Target BS/ABS has been rejected by the MS/AMS' Authenticator, the Target BS/ABS SHALL send HO_Rsp message with appropriate Failure Indication value to the Serving BS/ABS.

STEP 4

The Target BS/ABS 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/ABS does not support piggybacking of data path pre-registration signaling onto handover signaling, the Target BS/ABS may respond by initiating a data path pre-registration procedure with the Serving/Anchor ASN-GW.

STEP 5

The Serving BS/ABS sends a MOB_BSHO-RSP/AAI-HO-CMD message to the MS/AMS containing one or more potential Target BS/ABS's selected by the network for the MS/AMS to handover to.

STEP 6

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS(s) selected by the MS/AMS. 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/ABS(s) stops timer $T_{R6\_HO\_Rsp}$.

4.7.2.1.4 HO Preparation Scenario 4: Authenticator ASN-GW co-located with Serving and Relay ASN-GW (Scenario 4)

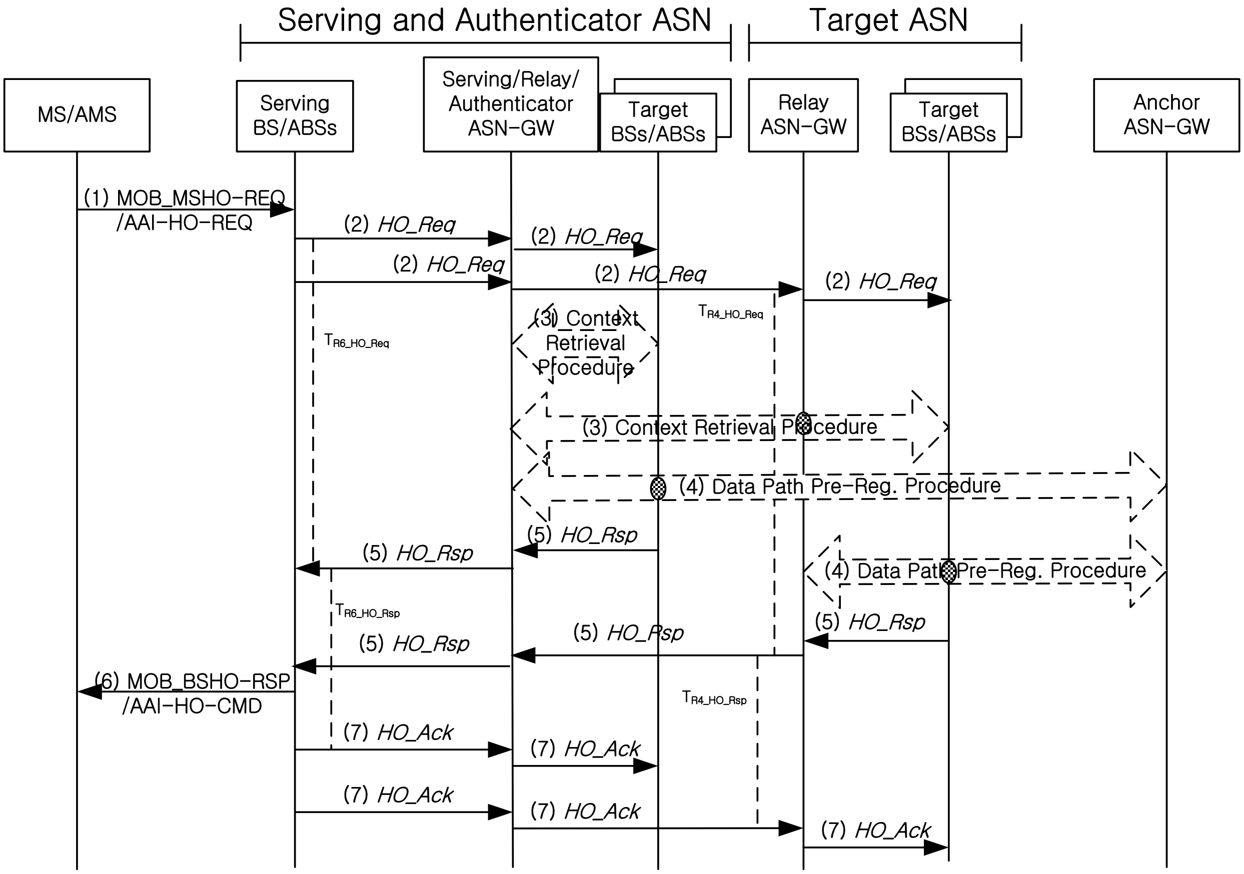


Figure 4-89 – Successful HO Preparation Phase, Scenario 4

STEP 1

The MS/AMS initiates a handover by sending a MOB-MSHO_REQ/AAI-HO-REQ message to the Serving BS/ABS which includes one or more candidate Target BS/ABS's.

STEP 2

The Serving BS/ABS sends a *HO_Req* message to each potential Target BS/ABS 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/ABS SHALL silently discard a duplicate MOB_MSHO-REQ/AAI-HO-REQ from an MS/AMS, if it has already initiated a HO preparation phase for this MS/AMS which is still ongoing. If a Serving BS/ABS receives such duplicate MOB_MSHO-REQ/AA-HO-REQ from an MS/AMS, it SHALL not propagate the request further in to the network.

The Serving BS/ABS sends a *HO_Req* message to the Target BS/ABS where the Serving BS/ABS starts timer $T_{R6\_HO\_Req}$ and the Target Relay ASN-GW starts $T_{R4\ HO\ Req}$. The Serving BS/ABS may send the message to multiple Target BS/ABS's for the potential handover. The Relay ASN-GW relays each *HO_Req* message to the corresponding Target BS/ABS.

STEP 3

The Target BS/ABS(s) requests AK context for the MS/AMS by initiating a Context Retrieval 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/ABS(s) may choose to defer this procedure to the handover action phase.

STEP 4

The Target BS/ABS(s) may initiate pre-establishment of a data path for the MS/AMS 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/ABS 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/ABS(s) MAY choose to defer this procedure to the handover action phase.

STEP 5

The Target BS/ABS(s) sends a *HO_Rsp* message to the Serving BS/ABS to acknowledge the handover request where Serving BS/ABS starts timer $T_{R6\_HO\_Rsp}$. The Relay ASN-GW relays the *HO_Rsp* messages to the Serving BS/ABS and starts $T_{R4\ HO\ Rsp}$. Upon receipt of the *HO_Rsp* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Req}$.

In the case Target BS/ABS 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/ABS sends a MOB_BSHO-RSP/AAI-HO-CMD message to the MS/AMS containing one or more potential Target BS/ABS's selected by the network for the MS/AMS to handover.

STEP 7

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS(s), selected for the MS/AMS. The Relay ASN-GW relays the *HO_Ack* message(s) to the corresponding Target BS/ABS(s). Upon receipt of the *HO_Ack* message, the Target BS/ABS(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/AAI_HO_CMD to the MS/AMS.

4.7.2.1.6 Network-Initiated Handover Scenario 1: AK Context Retrieval and Path Pregistraton Initiated by Target BS

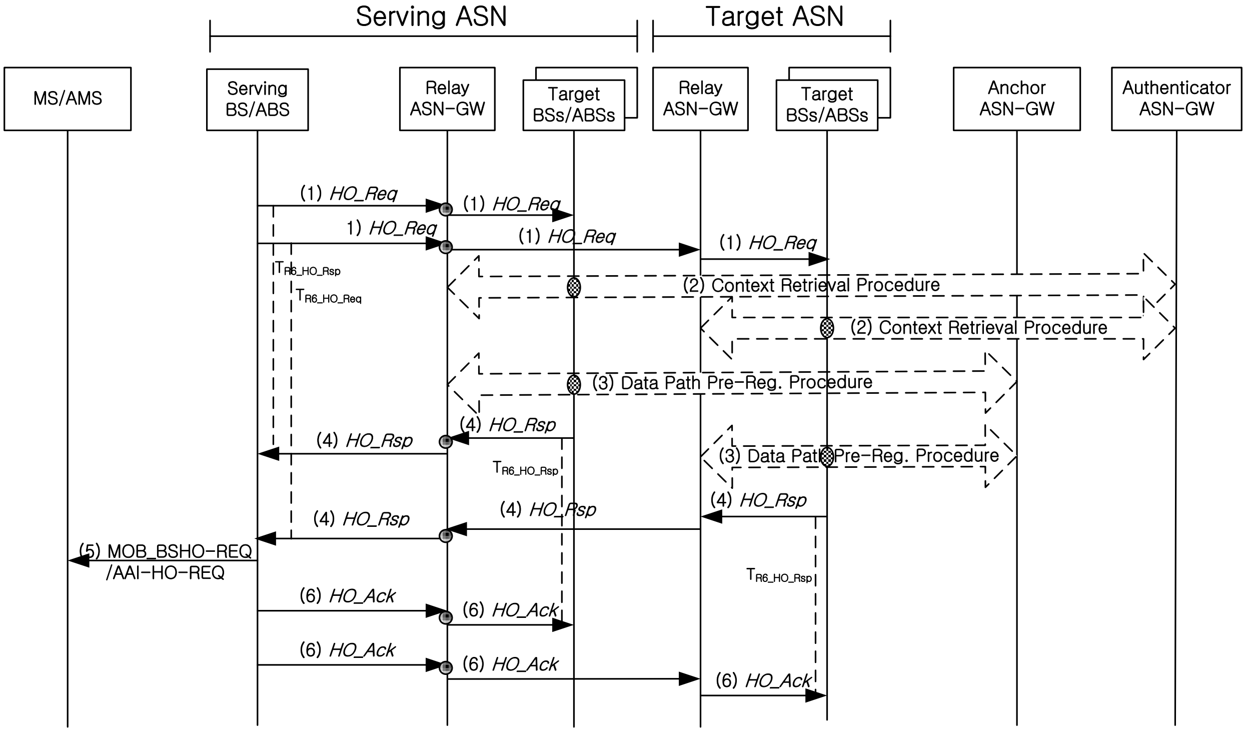


Figure 4-90 – Successful HO Preparation Phase Network Initiated HO Scenario 1

STEP 1

The Serving BS/ABS sends a *HO_Req* message to one or more Target BS/ABS'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/ABS.

STEP 2

The Target BS/ABS(s) requests AK context for the MSAMS by initiating a Context Retrieval 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/ABS initiates a Context Retrieval procedure with the Serving ASN-GW.

Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the handover action phase.

STEP 3

The Target BS/ABS(s) may initiate pre-establishment of a data path for the MS/AMS with the Anchor ASN after receiving *HO_Req* message. It can be initiated, if the Serving BS/ABS 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/ABS(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/ABS will be responded by the *Path_Prereg_Rsp* message with an appropriate failure indication.

Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the handover action phase.

STEP 4

The Target BS/ABS(s) sends a *HO_Rsp* message to the Serving BS/ABS to acknowledge the handover request. Relay ASN-GW relays the message to the Serving BS/ABS 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/ABS sends a MOB_BSHO-REQ/AAI-HO-CMD message to the MS with the Mode TLV set to 0b000 (HO Request)/0b00 (HO Command) and containing one or more potential Target BS/ABS's selected by the network for the MS/AMS to handover to. See IEEE 802.16e section 6.3.2.3.52/IEEE 802.16m section 16.x.x.

STEP 6

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS(s) selected for the MS/AMS. The Relay ASN-GW relays the R6 *HO_Ack* message(s) to the corresponding Target BS/ABS(s). Upon receipt of the *HO_Ack* message, the Target BS/ABS(s) stops timer $T_{R6\_HO\_Rsp}$.

Figure 4-91 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.

4.7.2.1.7 Network-Initiated Handover Scenario 2: Anchor ASN-GW Collocated with Serving ASN-GW and Path Pre-Registration Piggybacked onto HO Control messages

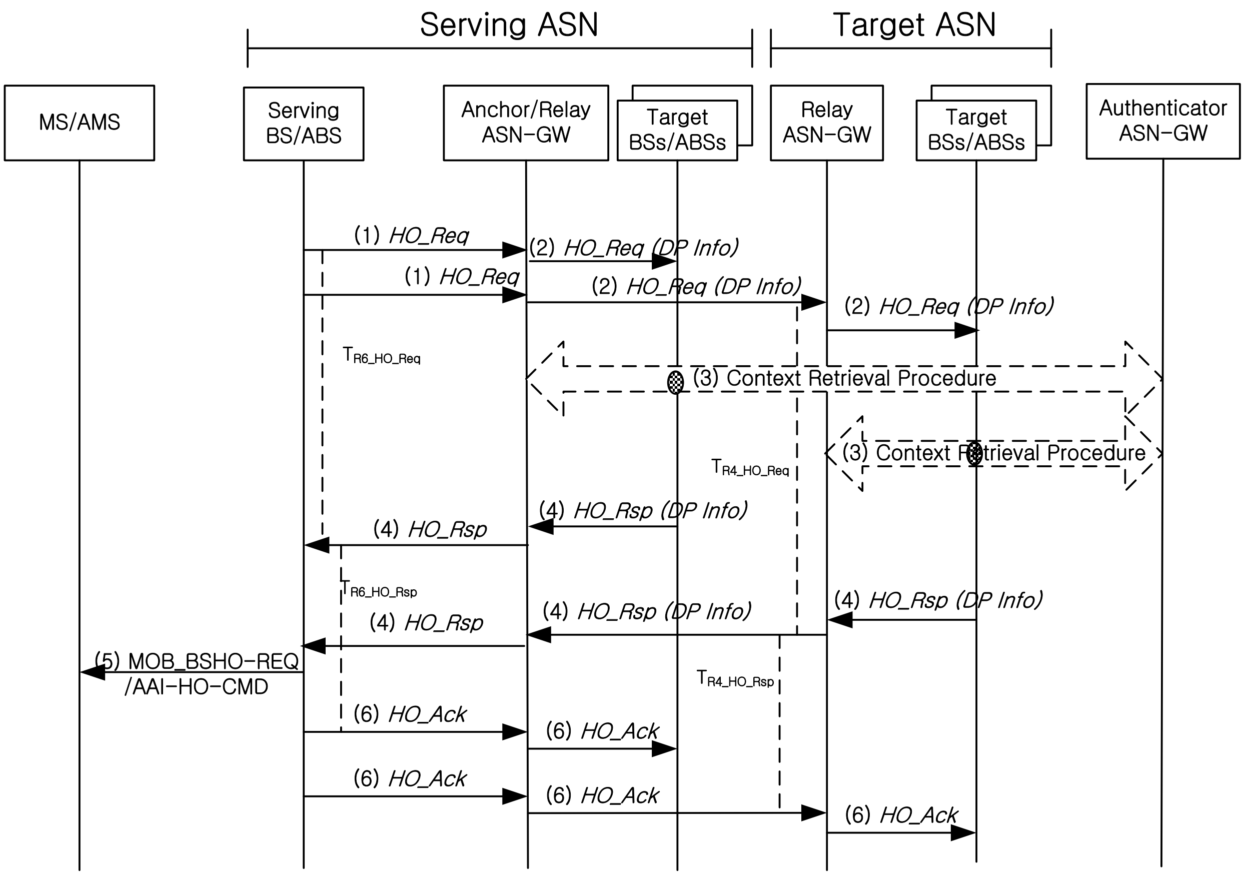


Figure 4-91 – Successful HO Preparation Phase, Network Initiated HO Scenario 2

STEP 1

The Serving BS/ABS initiates a handover by sending a *HO_Req* message to each potential Target BS/ABS 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/ABS may send the message to multiple Target BS/ABS'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/ABS, the Serving ASN-GW appends a *HO_Req* message with Data Path Info TLV to the Target BS/ABS.

STEP 3

The Target BS/ABS(s) requests AK context for the MS/AMS by initiating a Context Retrieval 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/ABS initiates a Context Retrieval procedure with the Serving ASN-GW. Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the handover action phase.

If AK context request for the particular Target BS/ABS has been rejected by the MS/AMS' Authenticator, the Target BS/ABS SHALL reject the handover request by sending *HO_Rsp* message with appropriate Failure Indication value to the Serving BS/ABS.

STEP 4

The Target BS/ABS 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/ABS does not support piggy backing of data path pre-registration signaling onto handover signaling, the Target BS/ABS may respond by initiating a Data Path Pre-Registration procedure with the Serving/Anchor ASN-GW.

STEP 5

The Serving BS/ABS sends a MOB_BSHO-REQ/AAI-HO-CMD message to the MS/AMS containing one or more potential Target BS/ABS's selected by the network for the MS/AMS to handover to.

STEP 6

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS(s) selected by the MS/AMS 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/ABS(s) stops timer $T_{R6\_HO\_Rsp}$.

4.7.2.1.8 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/ABS or Anchor ASN-GW when supporting Data Integrity BS buffer switching method via ASN-GW, initiating pre-registration of the data path for an MS/AMS, 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 or BS/ABS when supporting Data Integrity BS buffer switching method via ASN-GW, responding to pre-establishment of the data path for an MS/AMS, 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/ABS requesting context for a specific MS/AMS, 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/ABS upon sending the R6 HO_Req message for an MS/AMS to a Target BS/ABS and is stopped upon receiving a corresponding R6 HO_Rsp message from the Target BS/ABS.
- TR6_HO_Rsp: is started by a Target BS/ABS upon sending the R6 HO_Rsp message for an MS/AMS to a Serving BS/ABS and is stopped upon receiving a corresponding R6 HO_Ack message from the Serving BS/ABS.

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/AMS, 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/AMS, 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/AMS, 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/AMS 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/AMS to a Serving ASN-GW and is stopped upon receiving a corresponding R4 *HO_Ack* message from the Serving ASN.

Table 4-82 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 4-82 – 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

4.7.2.1.9 HO Preparation Stage Error Conditions

This section describes error conditions associated with the HO Preparation Phase.

4.7.2.1.9.1 Timer Expiry

Table 4-83 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 4-83.

Table 4-83 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{R6\_Path\_Pre\_Req}$	BS/ABS initiating Path Pre-Registration procedure	No action required
$T_{R6\_Path\_Pre\_Rsp}$	ASN-GW responding to *Path_Prereg_Req* message	No action required
$T_{R6\_Cntxt\_Req}$	BS/ABS Requesting context information	No action required
$T_{R6\text{-}HO\_Req}$	Serving BS/ABS	The BS/ABS may re-try HO to another Target BS/ABS. If no Target BS/ABS can be reached, it SHALL send MS/AMS a

		MOB_BSHO-RSP/AAI-HO-CMD with Mode set to 0b111
$T_{R6\_HO\_Rsp}$	Target BS/ABS	No action required
$T_{R4\_Path\_Pre\_Req}$	ASN initiating Data Path Pre-Registration procedure	No action required.
$T_{R4\_Path\_Pre\_Rsp}$	ASN responding to *Path_Prereg_Req* message	No action required.
$T_{R4\_Cntxt\_Req}$	ASN Requesting context info	No action required.
$T_{R4\_HO\_Req}$	Serving ASN	The Serving ASN may re-try HO to another Target ASN. If no Target ASN can be reached, the ASN SHALL send MS/AMS a MOB_BSHO-RSP/AAI-HO-CMD with Mode set to 0b111.
$T_{R4\_HO\_Rsp}$	Target ASN	No action required.

4.7.2.1.9.2 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/ABS SHALL stop timer $T_{R4\_Cntxt\_Req}$ or $T_{R6\_Cntxt\_Req}$ (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/ABS MAY resend the *Context_Req* message. If the Serving BS/ABS 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/ABS SHALL send a MOB_BSHO_RSP with mode = 0b111 to the MS/AMS. If the *Context_Req* message was triggered by the Target BS/ABS, then upon receipt of the *Context_Rpt* message with Failure Indication TLV, the Target BS/ABS MAY resend the *Context_Req* message. If the Target BS/ABS does not resend the *Context_Req* message or if subsequent attempts are also unsuccessful, then the Target BS/ABS SHALL send a *HO_Rsp* message with suitable error code included in the Result Code TLV.

4.7.2.1.9.3 HO_Rsp Error

Upon receipt of the *HO_Req* message, if the Target BS/ABS 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/ABS SHALL stop $T_{R6\text{-}HO\_Request}$ (if running). The Serving BS/ABS MAY re-send the *HO_Req* message to a different Target BS/ABS. If the Serving BS/ABS does not re-send the *HO_Req* message, of if all subsequent Target BS/ABSs cannot support the HO, in the case of MS Initiated handover, the Serving BS/ABS SHALL send either a MOB_BSHO_RSP with mode = 0b111 or a AAI-HO-RSP with mode=0b10 to the MS/AMS.

4.7.2.1.9.4 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 $T_{R4\text{-}DP\_Pre\text{-}Reg}$ and the BS/ABS SHALL stop $T_{R6\text{-}DP\_Pre\text{-}Reg}$ (if running) after the R6 *Path_Rsp* is received.

4.7.2.2 HO Action Phase[11]

If the MS/AMS accepts one of the Target BS/ABSs offered by the Serving BS/ABS in the MOB_BSHO-RSP/AAI-HO-CMD (MS initiated) or MOB_BSHO-REQ/AAI-HO-CMD (network initiated) message to handover to, the MS/AMS sends either a MOB_HO-IND message with HO_IND_type TLV set to 0b00 or a AAI-HO-IND message with HO Event Code set to 0b00 to the Serving BS/ABS in which it specifies which of the Target BS/ABSs offered by the Serving BS/ABS has been selected for the handover. If the MS accepts a Target BS/ABS offered to it by the Serving BS/ABS for handover, the MOB_HO-IND/AAI-HO-IND message is the last message the MS/AMS sends to the Serving BS/ABS. After sending MOB_HO-IND/AAI-HO-IND the MS/AMS starts ranging at the selected Target BS/ABS.

Upon receiving a MOB_HO-IND/AAI-HO-IND from the MS/AMS, indicating acceptance by the MS to handover to a Target BS/ABS offered by the Serving BS/ABS in the MOB_BSHO-RSP/AAI-HO-CMD (MS initiated) or MOB_BSHO-REQ/AAI-HO-CMD (network initiated) message, the Serving BS/ABS SHALL generate a *HO_Cnf* message and send it to the Target BS/ABS as shown in Figure 4-92.

For a handover from an ABS to another ABS, if the AAI-HO-CMD message sent to an AMS during the HO Preparation phase contains only one candidate Target ABS which is accepted for the handover also by the AMS, the AMS shall move to the Target ABS without sending an AAI-HO-IND to the serving ABS. In that case, the Serving BS/ABS SHALL generate a *HO_Cnf* message and send it to the Target BS/ABS at the Disconnect Time specified in the AAI-HO-CMD message.

The *HO_Cnf* message includes the "most recent MAC context" at the Serving BS/ABS. The Target BS/ABS SHALL complete the 2-way transaction by sending the *HO_Ack* to the Serving BS/ABS.

Upon receiving *HO_Cnf* message with the value for the HO_Indication type which is not set to "Cancel", the Target BS/ABS MAY retrieve the AK Context if this information was not retrieved or delivered during the Handover Preparation Phase. This call flow scenario (subsequently referred to as Scenario 1) is shown in Figure 4-92.

If the data path between the Anchor ASN-GW and the Target BS/ABS was not pre-established at the Preparation Phase, it MAY be pre-established after receiving *HO_Cnf* message and before the MS completes Network Re-Entry at the Target BS/ABS. In this case the Target BS/ABS initiates Data Path Pre-Registration. *Path_Prereg_Req/Rsp* message may include Data Delivery Trigger TLV in the SF Info. If this TLV is included and set to 1 it triggers immediate delivery of data for the specified Service Flow.

The data paths between the Anchor ASN-GW and the Target BS/ABS SHALL be established via Data Path Registration procedure after the MS/AMS arrives at the Target BS/ABS. The instance of "MS arrival" at the Target BS/ABS could be marked by a mobile initiated ranging, Network Entry completion or Network Re-Entry[12].

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 MSID. In such case a two-way Data Path Registration handshake will follow since the Data-Path Pre-registration process had been completed. 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; *Path_Reg_Req* and *Path_Reg_Rsp* 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 R4/R6 *Path_Reg_Req* and *Path_Reg_Rsp* messages SHALL convey all parameters relevant for the setup of Data

[11] This section describes handover control procedures which are applicable to handovers occurring between two Legacy BSs or between two Advanced BSs. For the handover control procedures between a Legacy BS and an Advanced BS, refer to subsection 4.7.4.

[12] 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.

Paths. In this case the R4/R6 *Path_Reg_Ack* message SHALL be sent in response to R4/R6 *Path_Reg_Rsp* message (i.e., three-way handshake).

After the HO completion, any SFs that have failed in establishing a data path SHALL be regarded as dropped and SHALL be released by the Anchor ASN-GW.

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 BS/ABSs that have not been selected for the final handover target. Also, the Anchor ASN-GW MAY initiate de-registration of the data path between itself and the (old) Serving BS/ABS.

If the Serving BS/ABS determines that the MOB_HO-IND/AAI-HO-IND message was not received from the MS/AMS due to a communication loss with the mobile[13] for example upon expiration of an internal timer[14], the Serving BS/ABS may send a *HO_Cnf* message (value for the HO_Indication type TLV should be set to a "Unconfirmed"- and latest MAC context from the MS) to Target BS/ABSs the MS/AMS may choose to handover to via Relay ASN-GW. The *HO_Cnf* message may be sent to Target BS/ABS(s) included in the MOB_BSHO-REQ/AAI-HO-CMD or MOB_BSHO-RSP/AAI-HO-CMD messages. The *HO_Cnf* message may also be sent to Target BS/ABSs which were not notified of a potential impending handover from the MS/AMS during the HO preparation phase and to Target BS/ABSs which were not included in the MOB_BSHO-REQ/AAI-HO-CMD or MOB_BSHO-RSP/AAI-HO-CMD messages. The *HO_Cnf* message includes the HO_Indication Type TLV set to "Unconfirmed" and latest MAC context for the MS. When sent to Target BS/ABSs which weren't previously notified of an impending handover from the MS during the HO preparation phase, the *HO_Cnf* message SHALL also include the Authenticator GW ID or AK context, and Anchor GW ID information. Upon sending the *HO_Cnf* message to the candidate Target BS/ABS(s), the Serving BS/ABS SHALL stop all the downlink and uplink scheduling for the data transmission and reception from the MS/AMS respectively.

Upon sending the *HO_Cnf* message, if the Resource_Retain flag was not set, the Serving BS/ABS SHALL discard all MS/AMS's connections resource information including the MAC state machine and all outstanding buffered PDUs, else the Serving BS/ABS SHALL retain the connections, MAC state machine and PDUs associated with the MS/AMS for service continuation until the expiration of Resource Retain Timer.

The Serving BS/ABS SHALL release all MAC context and MAC PDUs associated with the MS/AMS upon reception of a *HO_Complete* message from the Target ASN indicating MS/AMS completed a Network re-entry at the Target BS/ABS.

The *HO_Cnf* message may be delayed in the backbone network and arrive after the MS/AMS completes Network Re-Entry. If the R6 *HO_Cnf* message is not received by the Target BS/ABS until the MS/AMS appears at the Target BS/ABS, the Target BS/ABS 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/ABS SHALL perform the Data Path Registration procedure.

Immediately after the MS/AMS 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/ABS received with *Context_Rpt* from the Authenticator BS/ABS. However if the Target BS/ABS in the Target ASN receives and authenticates an RNG-REQ/AAI-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

[13] MOB_HO-IND/AAI-HO-IND message could be lost over the air or not sent by the MS/AMS because it didn't receive the MOB_BSHO-RSP/AAI-HO-CMD message from the BS/ABS in the MS initiated handover case, or it didn't receive the MOB_BSHO-REQ/AAI-HO-CMD from the BS/ABS in the network initiated handover case.

[14] For example, $T_{\text{MOB\_HO\_IND/AAI-HO-IND.}}$

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/ABS is completed, the Target BS/ABS SHALL send a *HO_Complete* message to the Serving BS/ABS to provide an accurate HO indication and expedite the resource release in the Serving BS/ABS. The Serving BS/ABS SHALL complete the 2-way transaction by sending the *HO_Ack*. Upon receiving the *HO_Complete* message, if the Serving BS/ABS did not yet release resources at the unselected Target BS/ABS(s), the Serving BS/ABS SHALL release the resources at the unselected Target BS/ABSs by sending the *HO_Cnf* message with Cancel indication. At this point the Serving BS/ABS SHOULD initiate Data Path De-registration procedure with the Anchor ASN-GW unless the de-registration procedure has already been initiated by the Anchor ASN-GW.

If the Target BS/ABS can't retrieve the necessary context due to error code "no record found" from the Serving BS/ABS or the Authenticator ASN-GW, it SHALL notify MS/AMS to conduct full network re-entry.

The *HO_Cnf* message with 'cancel' type may be sent to all candidate Target BS/ABSs that were not selected as a target for handover. The candidate BS/ABSs may initiate the Data Path release procedure after receiving this message, if they have completed the Path Pre-registration procedure during the Handover Preparation phase.

Unselected candidate Target BS/ABS 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/AMS rejects the Target BS/ABS(s) offered by the Serving BS/ABS in the MOB_BSHO-RSP/AAI-HO-CMD (MS initiated handover) or MOB_BSHO-REQ/AAI-HO-CMD (network initiated handover) message for the MS/AMS to handover to by sending either a MOB_HO-IND message with HO_IND_type TLV set to 0b10 or an AAI-HO-IND message with HO Event Code set to ob01 to the Serving BS/ABS, the Serving BS/ABS notifies the candidate Target BS/ABS previously notified of a potential handover from the MS/AMS in the handover preparation phase by sending a *HO_Cnf* message with a cancellation indication.

If the Serving BS/ABS offers a new Target BS/ABS candidate for the MS/AMS to handover to, it first notifies the Target BS/ABS(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/AAI-HO-CMD (if MS initiated handover described in section 4.7.2.1.4) or MOB_BSHO-REQ/AAI-HO-CMD (if network initiated handover described in section 4.7.2.1.5) message containing the new Target BS/ABS offered to the MS/AMS for handover.

The MS/AMS may be forced to perform a handover by sending either a MOB_HO-IND message with HO_IND_type set to 0b00 (Serving BS release) or an AAI-HO-IND message with HO Event Code set to 0b01 but including a preferred Target BS/ABS which was not offered by the Serving BS/ABS in the MOB_BSHO-RSP/AAI-HO-CMD or MOB_BSHO-REQ/AAI-HO-CMD message for the MS/AMS 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/ABS Sends HO_Cnf to Target BS/ABS

The following call flow describes a successful inter-ASN handover action scenario where the Target BS/ABS receives the *HO_Cnf* message from the Serving BS/ABS, and the Serving BS/ABS receives MOB_HO-IND/AAI-HO-IND and sends the *HO_Cnf* message to the Target BS/ABS (via Relay ASN-GW). The call flow also addresses the case where the Target BS/ABS receives the HO_Cnf message from the Serving BS/ABS but the Target BS/ABS was not notified of a potential impending handover from the MS during the HO preparation phase and was not included in the MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD messages.

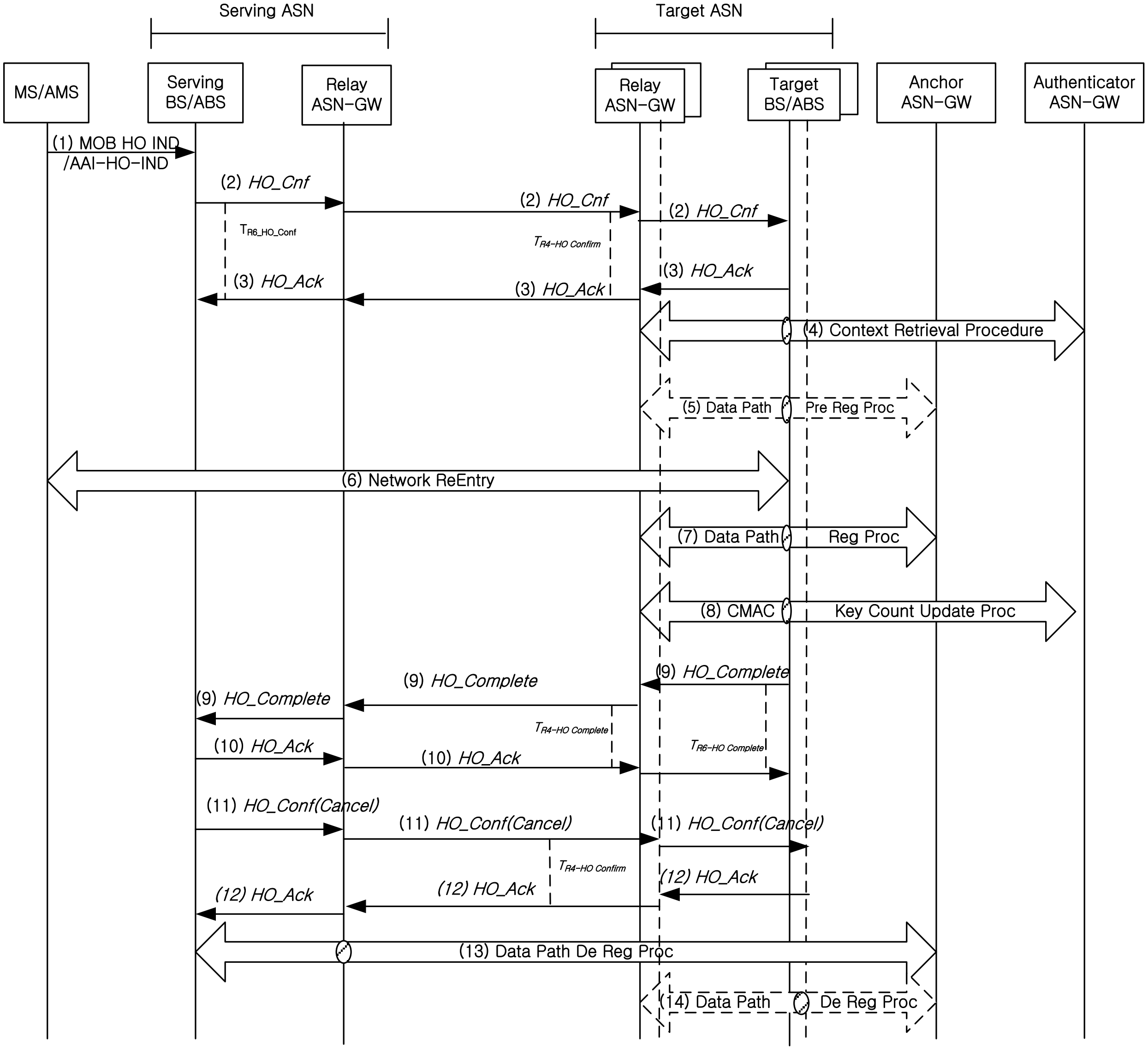


Figure 4-92 – Successful HO Action Phase, Scenario 1

STEP 1

The MS/AMS sends a MOB_HO-IND/AAI-HO-IND message to the Serving BS/ABS to initiate a handover to one of the Target BS/ABSs proposed or selected by the Serving BS/ABS in the Handover Preparation phase or potentially, in line with [13], [105], to a Target BS/ABS which has not been proposed by the Serving ASN-GW in the Handover Preparation phase.

In case that an AMS performs a handover between two ABSs and the AAI-HO-CMD message sent to an AMS during the HO Preparation phase contains only one candidate Target ABS which is accepted for the handover also by the AMS, the AMS shall move to the Target ABS without sending an AAI-HO-IND to the serving ABS.

STEP 2

Upon reception of the MOB_HO-IND/AAI-HO-IND message or upon expiration of the Action Time, the Serving BS/ABS sends a *HO_Cnf* message to the selected Target BS/ABS and starts timer $T_{R6\_HO\_Conf}$. The Serving BS/ABS MAY also send *HO_Cnf* message with the value of the HO_Indication type set to "Cancel" to all unselected Target BS/ABS(s) and clear the MS context anytime after receiving MOB_HO-IND/AAI-HO-IND message. – In case that the selected Target BS/ABS was not notified of a potential impending handover from the MS/AMS during the handover preparation phase and its Target BS/ABSs were not included in the MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD 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/ABS sends a *HO_Ack* message to the Serving BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R4/R6. Upon receipt of the *HO_Ack* message, the Serving BS/ABS 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/AMS was not requested during the Handover Preparation phase, the Target BS/ABS requests AK context for the MS/AMS by initiating a Context Retrieval 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/AMS initiates network re-entry with the Target BS/ABS by sending an RNG-REQ/AAI-RNG-REQ.

The Target BS/ABS responds with an RNG-RSP/AAI-RNG-RSP and the MS/AMS and the Target BS/ABS complete Network Reentry..

STEP 7

Target BS/ABS initiates Data Path Registration procedure (see section 4.12.3) with the Anchor ASN-GW. 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/ABS 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/AMS.

STEP 9

Upon completion of network re-entry, the Target BS/ABS SHALL sends a *HO_Complete* message to the Serving BS/ABS 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/ABS. Upon receipt of the *HO_Complete* message, the Serving BS/ABS releases the MS context.

STEP 10

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Comp}$.

STEP 11

Upon receiving the HO_Complete message, if Serving BS/ABS did not send *HO_Cnf* message with the value of the HO_Indication type set to "Cancel" to all unselected Target BS/ABS(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/ABS(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/ABS sends a *HO_Ack* message to the Serving BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Conf}$.

STEP 13

Upon receiving the HO_Complete message, if the Serving BS/ABS has not deleted the data path previously and still has a data path with Anchor ASN-GW, the Serving BS/ABS 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/ABS, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure (see section 4.12) with the old Serving BS/ABS.

STEP 14

The Anchor ASN-GW SHALL de-register all the pre-registered data paths with the unselected Target BS/ABSs.

4.7.2.2.2 Handover Action Scenario 2: HO_Cnf not Received at Target BS/ABS

The following call flow describes a successful inter-ASN Handover Action scenario where the MOB_HO-IND/AAI-HO-IND sent by the MS/AMS to the Serving BS/ABS was lost over the air and not received by the Serving BS/ABS, and/or the *HO_Cnf* message sent by the Serving BS/ABS to the Target BS/ABS was either delayed or not received. The MS/AMS completes network re-entry at one of the Target BS/ABSs selected by the Serving BS/ABS during the Handover Preparation phase.

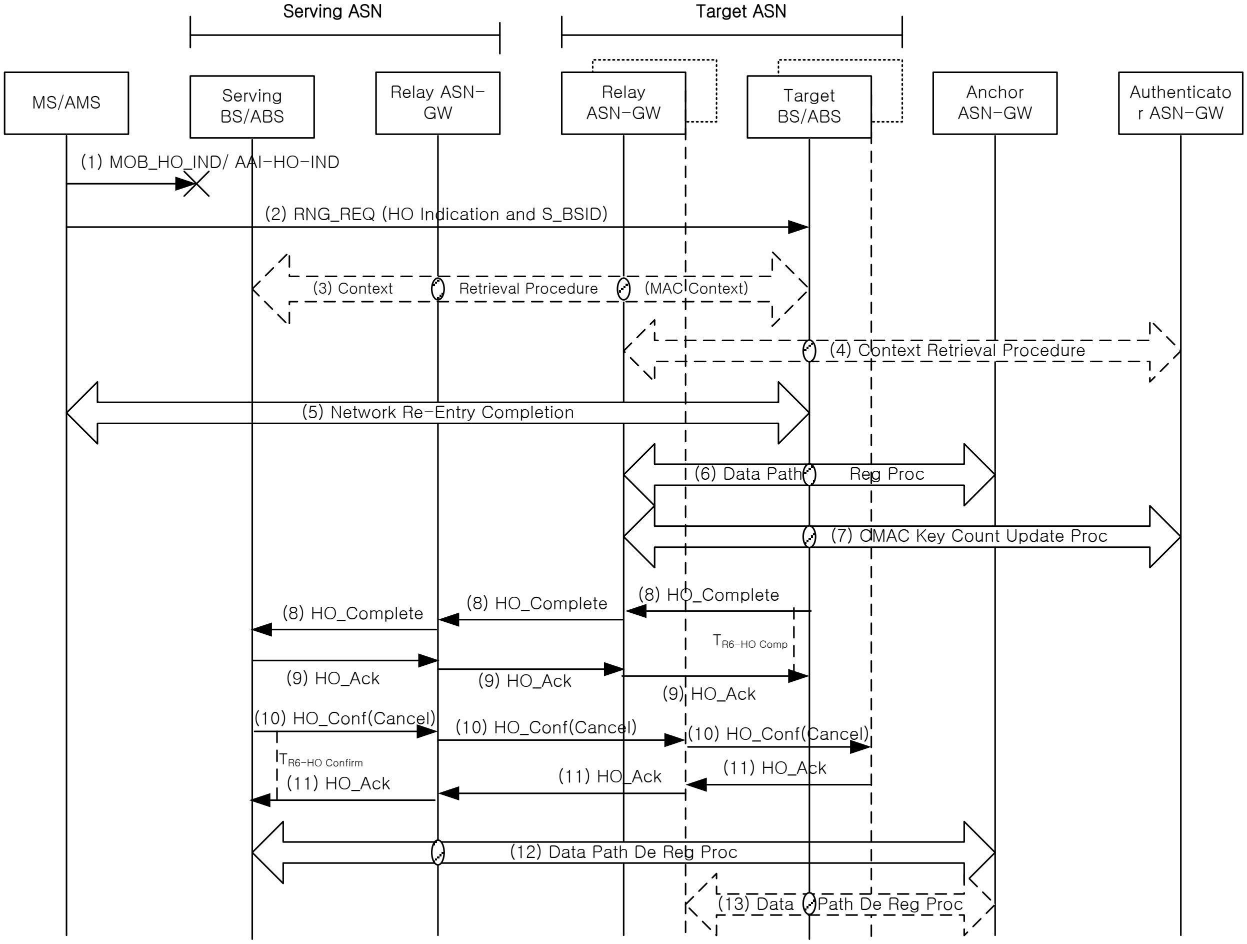


Figure 4-93 – Successful HO Action Phase, Scenario 2

STEP 1

The MOB_HO-IND/AAI-HO-IND message is sent by the MS/AMS to the Serving BS/ABS and lost over the air or not properly received by the ServingBS/ABS.

STEP 2

The MS/AMS sends an RNG-REQ/AAI-RNG-REQ message with HO_Indication and the Serving BS/ABS ID information to one of the Target BS/ABSs that was indicated by the Serving BS/ABS during the Handover Preparation phase. If the Serving BS/ABS ID was not included, an initial network entry is required and initial network entry procedures SHALL be followed.

STEP 3

The Target BS/ABS initiates a Context Retrieval procedure (see section 4.12) with the Serving BS/ABS to retrieve the latest MAC context for the MS/AMS. 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/ABS requests AK context for the MS/AMS by initiating a Context Retrieval procedure (see section 4.12) with the Authenticator ASN-GW.

STEP 5

After completing the retrieval of the MS context, the Target BS/ABS sends Ranging Response to the MS/AMS. The MS/AMS and Target BS/ABS complete the network Re-entry including the exchange of the required parameters (i.e., SBC-Req/Rsp).

STEP 6

The Target BS/ABS 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 Retrieval procedure in step 2.

STEP 7

Upon successful completion of network re-entry, the Target BS/ABS 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/AMS.

STEP 8

Upon completion of network re-entry, the Target BS/ABS SHALL send a *HO_Complete* message to the Serving BS/ABS to notify the completion of the handover. Relay ASN-GW relays the *HO_Complete* message over R4/R6 to the Serving BS/ABS. Upon receipt of the *HO_Complete* message, the Serving BS/ABS releases MS context and starts timer $T_{R6\_HO\_Comp}$.

STEP 9

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R4/R6. Upon receipt of the *HO_Ack* message, the Target BS/ABS stops timer $T_{R6\_HO\_Comp}$.

STEP 10

The Serving BS/ABS may have already sent the *HO_Cnf* message with the HO_Indication type set to “Cancel” to some or all BS/ABSs. For all unselected Target BS/ABSs to which such message has not been sent yet, the Serving BS/ABS SHALL send such a message upon receipt of *HO_Complete* message in order to clear the MS context at Target BS/ABSs. When Serving BS/ABS 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/ABS sends an *HO_Ack* message to the Serving BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Conf}$.

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/ABS 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/ABS, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure with the old Serving BS/ABS.

STEP 13

The Anchor ASN-GW SHALL de-register all the pre-registered data paths with the other (not selected) Target BS/ABSs.

4.7.2.2.3 Handover Action Scenario 3: MOB_HO-IND not received at Serving BS/ABS

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/ABS was lost over the air and not received by the Serving BS/ABS. The MS completes network re-entry at one of the Target BS/ABS s selected by the Serving BS/ABS during the Handover Action phase, or a Target BS/ABS which wasn't notified of an impending handover from the MS/AMS 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/ABS 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 BS/ABSs (via Relay ASN-GW).

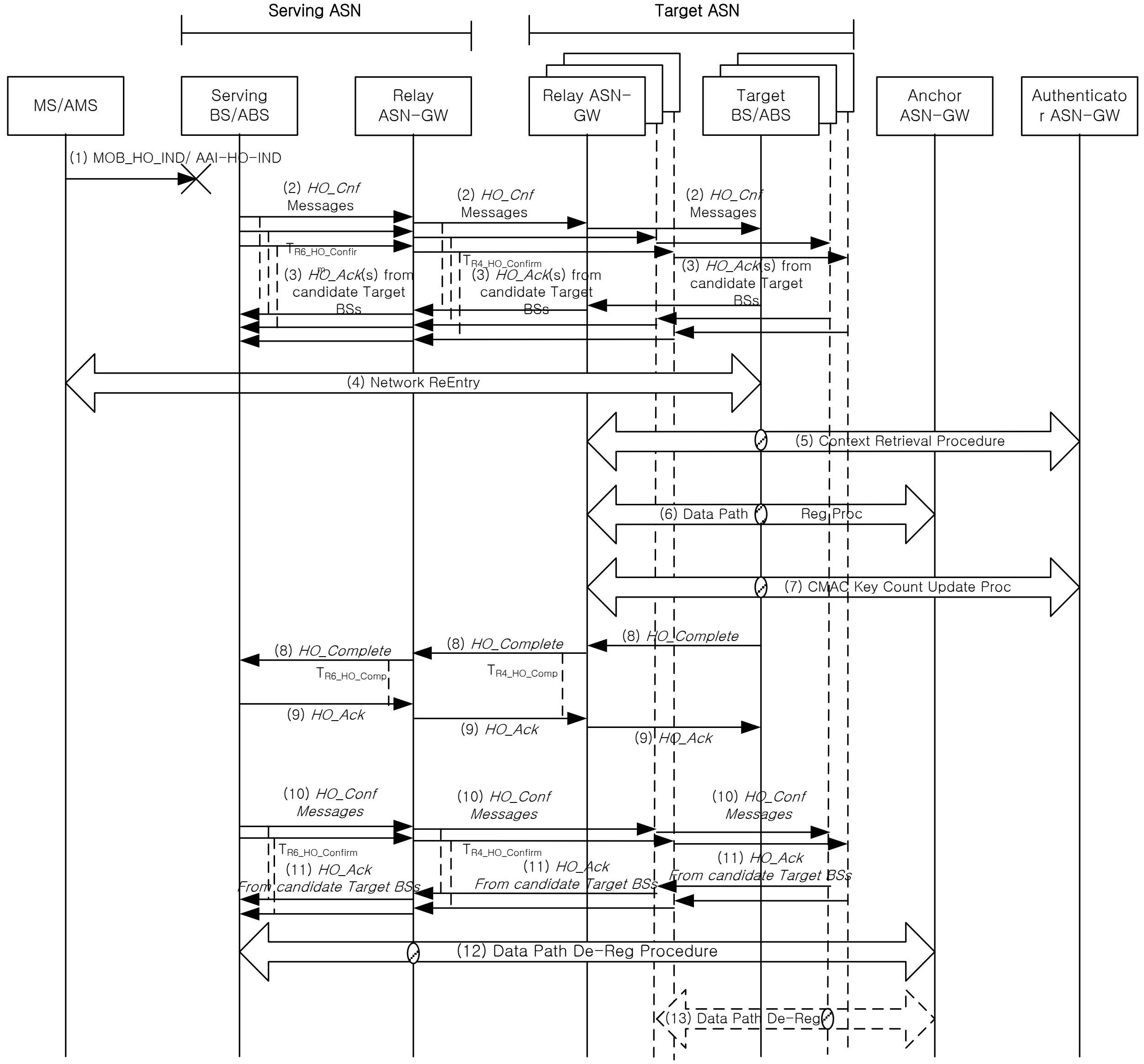


Figure 4-94 – Successful HO Action Phase, Scenario 3

STEP 1

The MOB_HO-IND/AAI-HO-IND sent by the MS/AMS to the Serving BS/ABS is lost over the air and not received by the Serving BS/ABS.

STEP 2

Upon expiration of internal timer at the Serving BS/ABS, the Serving BS/ABS sends a *HO_Cnf* message(s) with "Unconfirmed" type to the set of Target BS/ABS(s) controlling the candidate Target BS/ABS(s) which were indicated in the MOB_BSHO-RSP or MOB_BSHO-REQ or AAI-HO-CMD, and starts the $T_{R6\_HO\_Conf}$ timer. The Serving BS/ABS also sends *HO_Cnf* message to any candidate Target BS/ABSs the MS/AMS 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/ABS sends *HO_Ack* message to the Serving BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops the corresponding $T_{R6\_HO\_Conf}$ timer.

STEP 4

The MS/AMS completes network re-entry at one of the Target BS/ABSs selected by the Serving BS/ABS during the Handover Action phase, or at a Target BS/ABS notified of an impending handover from the MS/AMS after the Serving BS/ABS detects the loss of communication with the MS/AMS due to loss of the MOB_HO-IND/AAI-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/ABS requests AK context for the MS/AMS by initiating a Context Retrieval 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/ABS 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/ABS 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/AMS.

STEP 8

The Target BS/ABS SHALL send an *HO_Complete* message to the Serving BS/ABS 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/ABS releases the MS context and stops the Resource Retain Timer and starts timer $T_{R6\_HO\_Comp}$.

STEP 9

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS 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/ABS stops timer $T_{R6\_HO\_Comp}$.

STEP 10

The Serving BS/ABS may have already sent the *HO_Cnf* message with the HO_Indication type set to “Cancel” to some or all Target BS/ABSs. For all unselected Target BS/ABSs to which such message has not been sent yet, the Serving BS/ABS SHALL send such a message upon receipt of *HO_Complete* message in order to clear the MS context at Target BS/ABSs. When Serving BS/ABS sends the *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/ABS sends a *HO_Ack* message to the Serving BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Conf}$.

STEP 12

Upon receiving the *HO_Complete* message, if the Serving BS/ABS has not deleted the data path previously and still has a data path with Anchor ASN-GW, the Serving BS/ABS SHALL initiate Data Path De-Registration procedure with the Anchor ASN-GW. Upon completing the Data Path Registration procedure with the Target BS/ABS, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure with the old Serving BS/ABS.

STEP 13

The Anchor ASN-GW SHALL de-register all the pre-registered data paths with the other (not selected) Target BS/ABSs.

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/ABS during the Handover Action phase. The Target BS/ABS receives the *HO_Cnf* message from the Serving BS/ABS via the Relay ASN-GW.

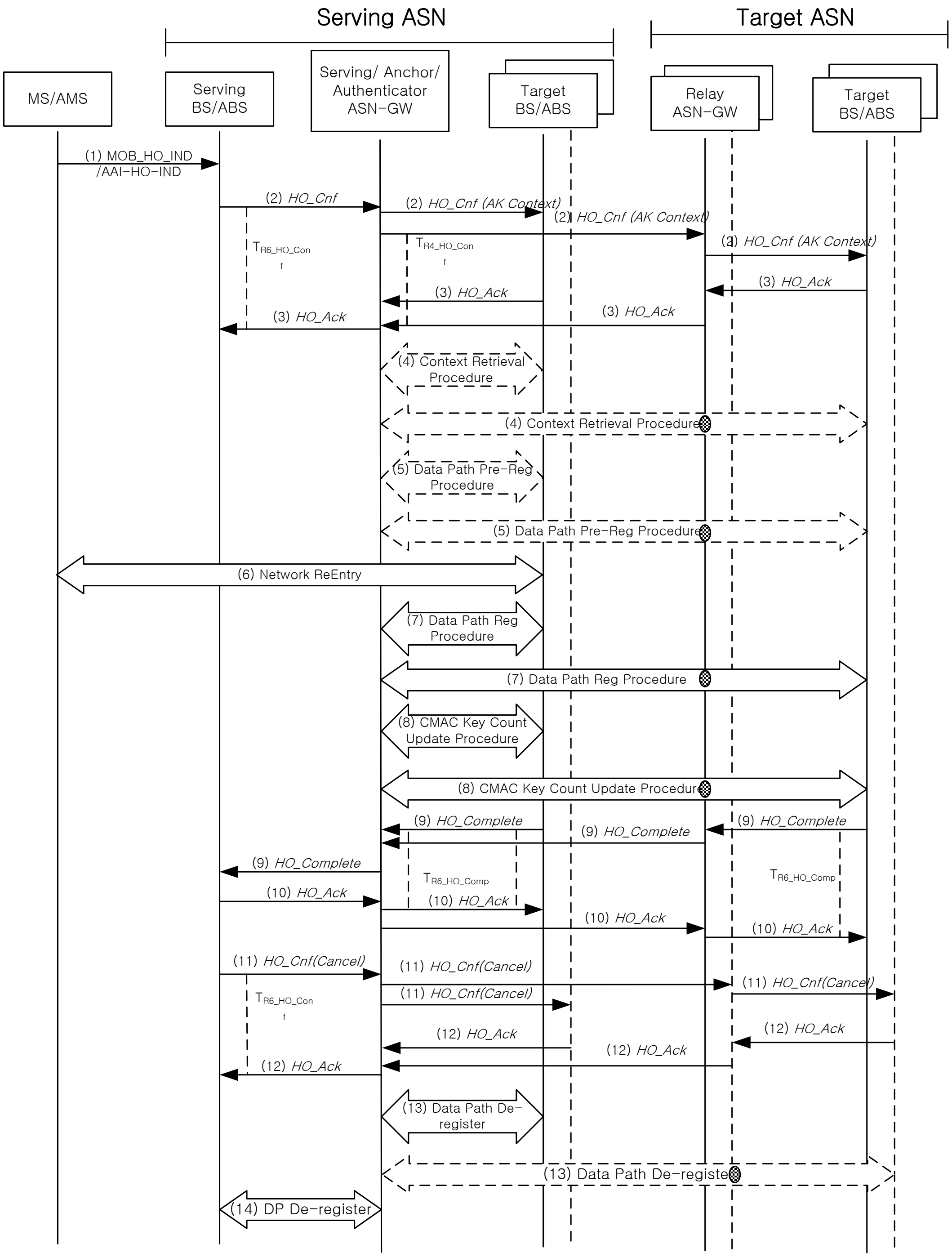


Figure 4-95 – Successful HO Action Phase, Scenario 4

STEP 1

The MS/AMS sends a MOB_HO-IND/AAI-HO-IND to the Serving BS/ABS to notify a handover to one of the Target BS/ABSs candidates selected by the Serving BS/ABS during the Handover Preparation phase.

In case that an AMS performs a handover between two ABSs and the AAI-HO-CMD message sent to an AMS during the HO Preparation phase contains only one candidate Target ABS which is accepted for the handover also by the AMS, the AMS shall move to the Target ABS without sending an AAI-HO-IND to the serving ABS.

STEP 2

Upon reception of the MOB_HO-IND/AAI-HO-IND or upon expiration of Action Time, the Serving BS/ABS sends an *HO_Cnf* message and starts timer $T_{R6\_HO\_Conf}$. Serving BS/ABS MAY also send an *HO_Cnf* message with the value of the HO_Indication type set to “Cancel” to all unselected Target BS/ABS(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/ABS, 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/ABS, the Anchor ASN-GW MAY send the piggybacked Data Path Info TLV with *HO_Cnf* message.

STEP 3

The Target BS/ABS sends an *HO_Ack* message to the Serving BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Conf}$.

STEP 4

If the Serving BS/ABS doesn’t support the piggybacked AK Context, the Target BS/ABS may initiate a Context Retrieval procedure with the Authenticator ASN-GW.

STEP 5

The Serving BS/ABS may initiate a Data Path Pre-Registration procedure (see section 4.12) with the Anchor ASN-GW if Data Path Pre-Registration did not occur. If the Target BS/ABS doesn’t support Anchor ASN-GW initiated Data Path Pre-Registration procedure, it may initiate the procedure on its own.

STEP 6

The MS/AMS initiates network re-entry with the Target BS/ABS.

STEP 7

If not already established, the Target BS/ABS 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/ABS 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/AMS.

STEP 9

Upon completion of network entry, the Target BS/ABS SHALL send a *HO_Complete* message to the Serving BS/ABS to acknowledge the completion of the handover start timer and starts timer $T_{R6\_HO\_Comp}$. Relay ASN-GW relays the *HO_Complete* message over R6/R4. Upon receipt of the *HO_Complete* message, the Serving BS/ABS SHALL release the MS context.

STEP 10

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4. Upon receipt of the *HO_Ack* message, the Target BS/ABS stops timer $T_{R6\_HO\_Comp}$.

STEP 11

Upon receiving the *HO_Complete* message, if the Serving BS/ABS did not send an HO_Cnf message with the value of the HO_Indication type set to "Cancel" to all unselected Target BS/ABS(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/ABS(s) to clear the MS context and starts timer $T_{R6\_HO\_Conf}$.

Relay ASN-GW relays the *HO_Complete* message over R6/R4.

STEP 12

The unselected Target BS/ABS sends a *HO_Ack* message to the Serving BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R4\_HO\_Conf}$.

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 BS/ABSs candidates.

STEP 14

The Serving/Anchor ASN-GW deregisters the data path with the (old) Serving BS/ABS.

4.7.2.3 HO Cancellation

HO Cancellation is a variant of HO Action Phase, when the Serving BS/ABS signals to one or more Target BS/ABS(s) that the HO is to be cancelled. The HO Cancellation will be invoked only if the Target BS/ABS 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 BS/ABSs that have not been chosen as the final HO Target by the MS or to all the Target BS/ABSs 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/AAI-HO-IND message with the indication to cancel the handover procedure; anytime after receipt of a MOB_HO-IND/AAI-HO-IND message with indication of a handover to the Target BS/ABS selected as part of preparationphase, or the HO_Complete message received by the Serving BS/ABS when the MS/AMS completes the network re-entry at the Target BS/ABS.

Note: The term "Unselected Target BS/ABS" in the following figures for various HO Cancellation scenarios refers to the Target BS/ABS that had been selected as the potential Target BS/ABS that the MS/AMS may handover to, and which includes at least one Target BS/ABS 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/ABS" Receives HO_Cnf from Serving BS/ABS

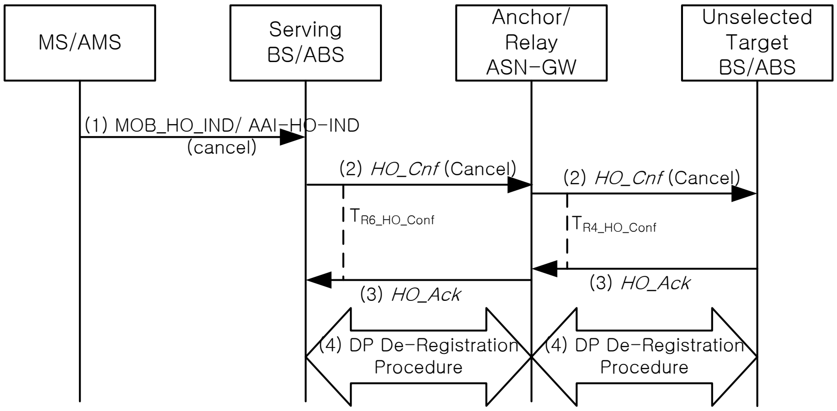


Figure 4-96 –HO Cancellation, Scenario 1

STEP 1

The MS/AMS sends MOB_HO_IND/AAI-HO-IND to the Serving BS/ABS. In the MOB_HO_IND/AAI-HO-IND, the MS/AMS indicates, that it decided to cancel the handover procedure, in this case, the selected Target BS/ABS is the Serving BS/ABS.

STEP 2

Receiving either the MOB_HO-IND with HO_IND_type set to 0b01: HO Cancel or the AAI-HO-IND with HO Event Code set to 0b11: HO Cancel causes the Serving BS/ABS to send *HO_Cnf* message with the value of the HO_Indication type set to "Cancel" to inform the previously selected potential Target BS/ABS(s) which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD message to de-allocate the reserved system resources that are prepared for the MS/AMS to handover. After sending the message, the Serving BS/ABS awaits for the *HO_Ack* message by starting the $T_{R6\_HO\_Cnf}$. If the timer expires, the Serving BS/ABS may re-send the *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS/ABS stops resending the *HO_Cnf*. The Target BS/ABS SHALL perform the local clean up if *HO_Cnf* is never received from the Serving BS/ABS. Relay ASN-GW relays the *HO_Ack* message over R6/R4 and starts $T_{R6/R4\_HO\_Cnf}$.

STEP 3

If the Target BS/ABS receives the *HO_Cnf* with HO_Indication type set to "Cancel", the Target BS/ABS sends *HO_Ack* to the Serving BS/ABS and releases the pre-allocated system resources, which are to support the MS/AMS handover. The Target BS/ABS may also initiate the Data Path De-Registration Procedure (section 4.12.4) towards the Anchor ASN-GW if a data path had been pre-established.

STEP 4

Upon expiry of the MS Context Retain Timer, the Serving BS/ABS may start the Data Path De-Registration Procedure (section 4.12.4) to the Anchor ASN-GW. Also the Anchor ASN-GW or unselected Target BS/ABS may start Data Path De-Registration Procedure (section 4.12.4) if data path had been established between them during the HO Preparation phase. The Data Path De-Registration message includes both normal data path and BS/ABS Buffer Switching data path if BS/ABS buffer switching method via Anchor ASN-GW is involved. If the MS/AMS is no longer attached to the Serving BS/ABS, the Serving BS/ABS SHALL release all the allocated system resource for the MS/AMS.

4.7.2.3.2 HO Cancellation Scenario 2: Serving and Anchor ASN-GW are not Collocated and "Unselected Target BS/ABS" receives HO_Cnf from Serving BS/ABS

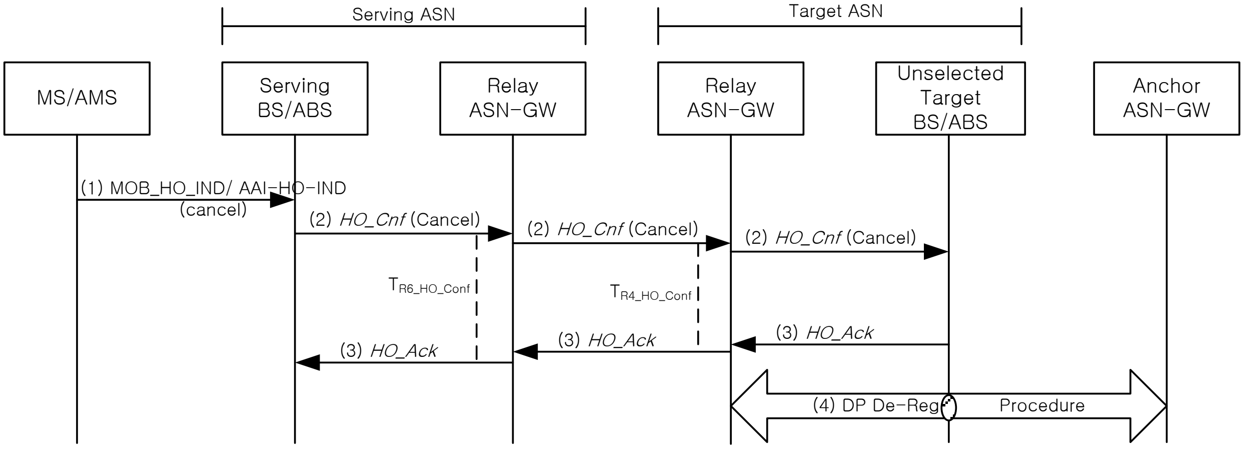


Figure 4-97 –HO Cancellation, Scenario 2

STEP 1

The MS/AMS sends MOB_HO-IND/AAI-HO-IND to the Serving BS/ABS. In the MOB_HO-IND/AAI-HO-IND, the MS/AMS indicates, that it decided to cancel the handover procedures. In this case, the selected Target BS/ABS is the Serving BS/ABS.

STEP 2

Receiving either the MOB_HO-IND with HO_IND_type set to 0b01: HO Cancel or the AAI-HO-IND with HO Event Code set to 0b11: HO Cancel causes the Serving BS/ABS to send *HO_Cnf* message with the value of HO_Indication type set to "Cancel" to inform the previously selected potential Target BS/ABS(s) which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD message to de-allocate the reserved system resources that are prepared for the MS/AMS to handover. After sending the message, the Serving BS/ABS awaits *HO_Ack* by starting the $T_{R6\_HO\_Cnf}$. Relay ASN-GW relays the message over R6/R4 and starts timer $T_{R6/R4\_HO\_Cnf}$. If the timer expires, the Serving BS/ABS may re-send the *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS/ABS stops resending the *HO_Cnf*. The Target BS/ABS SHALL perform the local clean up if *HO_Cnf* is never received from the Serving BS/ABS.

STEP 3

Target BS/ABS receives the *HO_Cnf* with HO_Indication type set to "Cancel". Target BS/ABS sends *HO_Ack* to the Serving BS/ABS and may release the pre-allocated system resources, which are to support the MS/AMS handover. Relay ASN-GW relays the message over R6/R4.

STEP 4

The Target BS and the Anchor ASN-GW may start the Data Path De-Registration Procedure (section 4.12.4) if data path had already been established between them. The Data Path De-Registration message includes both normal data path and BS/ABS Buffer Switching data path if BS/ABS Buffer Switching method via Anchor ASN-GW is involved. If the MS/AMS is no longer attached to the Serving BS/ABS, the Serving BS/ABS SHALL release all the allocated system resource for the MS/AMS.

4.7.2.3.3 HO Cancellation Scenario 3: A subset of the Target BS/ABS(s) does not Receive HO_Cnf(Cancel).

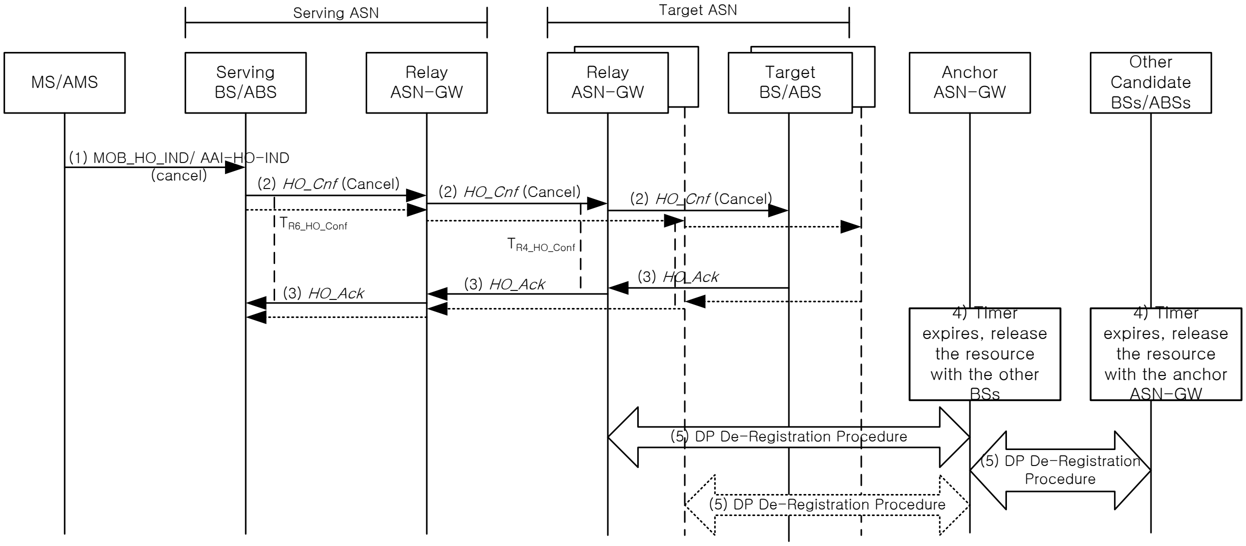

Serving ASN
Target ASN
MS/AMS
Serving BS/ABS
Relay ASN-GW
Relay ASN-GW
Target BS/ABS
Anchor ASN-GW
Other Candidate BSs/ABSs
(1) MOB_HO_IND/ AAI-HO-IND (cancel)
(2) HO_Cnf (Cancel)
(2) HO_Cnf (Cancel)
(2) HO_Cnf (Cancel)
TR6_HO_Conf
TR4_HO_Conf
(3) HO_Ack
(3) HO_Ack
(3) HO_Ack
4) Timer expires, release the resource with the other BSs
4) Timer expires, release the resource with the anchor ASN-GW
(5) DP De-Registration Procedure
(5) DP De-Registration Procedure
(5) DP De-Registration Procedure

Figure 4-98 – HO Cancellation, Scenario 3

STEP 1

The MS/AMS sends MOB_HO-IND/AAI-HO-IND to the Serving BS/ABS. In the MOB_HO-IND/AAI-HO-IND, the MS/AMS indicates, that it decided to cancel the handover procedures. In this case, the selected Target BS/ABS is the Serving BS/ABS.

STEP 2

Receiving either the MOB_HO-IND with HO_IND_type set to 0b01: HO Cancel or the AAI-HO-IND with HO Event Code set to 0b11: HO Cancel causes the Serving BS/ABS to send *HO_Cnf* message with the value of HO_Indication type set to "Cancel" to inform the previously selected potential Target BS/ABS(s) which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD message to de-allocate the reserved system resources including CMAC context that are prepared for the MS/AMS to handover. After sending the message, the Serving BS/ABS awaits *HO_Ack* by starting the $T_{R6\_HO\_Cnf}$. Relay ASN-GW relays the message over R6/R4 and starts timer $T_{R6/R4\_HO\_Cnf}$. If the timer expires, the Serving BS/ABS may re-send the *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS/ABS stops resending the *HO_Cnf*. The Target BS/ABS SHALL perform the local clean up if *HO_Cnf* is never received from the Serving BS/ABS.

STEP 3

The Target BS/ABS(s) sends a *HO_Ack* to the serving BS/ABS and releases the MS resources. Relay ASN-GW relays the message over R6/R4. Upon receipt of the *HO-Ack* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Cnf.}$

STEP 4

If one of the Target BS/ABSs does not receive the *HO_Cnf*, upon a timer expiry the Target BS/ABS releases the pre-allocated system resources, and if obtained the MS context, which are to support the MS/AMS handover.

STEP 5

After receiving HO_Cnf (Cancel) or after the timer associated with the pre-registered data path expires, the Target BS/ABS(s) may start the *Path_ Deregistration* Procedure (4.12.4), through the relay ASN-GW, to the Anchor ASN-GW if a data path had already been established between the Target BS/ABS(s) and the Anchor ASN-GW. The Data Path De-Registration message includes both normal data path and BS/ABS Buffer Switching data path if BS/ABS buffer switching method via Anchor ASN-GW is involved. If the MS/AMS is no longer attached to the Serving BS/ABS, the Serving BS/ABS SHALL release all the allocated system resource for the MS/AMS.

4.7.2.3.4 HO Cancellation Scenario 4: Serving BS/ABS receives HO_Complete

In this scenario the MS/AMS successfully completes the network re-entry procedure at a Target BS/ABS. Note that the Target BS/ABS where the MS re-entered may be different from the BS indicated in the MOB_HO_IND/AAI-HO-IND message at the start of the HO action phase.

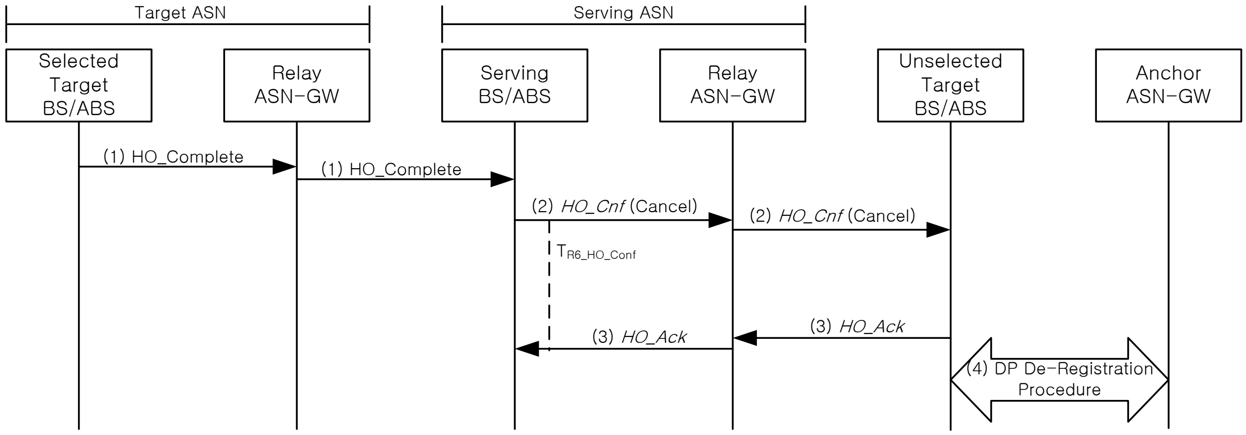


Figure 4-99 – HO Cancellation, Scenario 4

STEP 1

The BS/ABS where the MS/AMS completed network re-entry sends *HO_Complete* message to the Serving BS/ABS. Relay ASN-GW relays the message over R6/R4.

STEP 2

Receiving the *HO_Complete* message causes the Serving BS/ABS, (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/ABS(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/ABS(s) to de-allocate the reserved system resources that are prepared for the MS/AMS to handover. Relay ASN-GW relays the message over R6/R4 and starts timer $T_{R6/R4\_HO\_Cnf}$. After sending the message, the Serving BS/ABS awaits for the *HO_Ack* message by starting the $T_{R6\_HO\_Cnf}$. If the timer expires, the Serving BS/ABS may re-send the *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS/ABS stops resending the *HO_Cnf*. The Target BS/ABS SHALL perform the local clean up if *HO_Cnf* is never received from the Serving BS/ABS.

STEP 3

Each unselected Target BS/ABS sends *HO_Ack* to the Serving BS/ABS and releases the pre-allocated system resources, which are to support the MS/AMS handover. Relay ASN-GW relays the message over R6/R4. Upon the resource retain timer expiry, if the MS/AMS is no longer attached to the Serving BS/ABS, the Serving BS/ABS SHALL release all the allocated system resource for the MS/AMS.

STEP 4

If the Target BS/ABS still have a data path pre-established with the Anchor ASN-GW, the Target BS/ABS may also initiate the Data Path De-registration procedure (section 4.12.4). The Data Path De-Registration message includes both normal data path and BS/ABS Buffer Switching data path if BS/ABS buffer switching method via Anchor ASN-GW is involved.

Note:

If the Serving BS/ABS receives neither the MOB_HO_IND/AAI-HO-IND message nor the *HO_Complete* message, upon the expiration of the internal timer the Serving BS/ABS SHOULD send a *HO_Confirm*(cancel) message to all the candidate Target BS/ABSs.

4.7.2.4 MS Handover Rejection[15]

The following call flow describes the scenario when the MS/AMS rejects Target BS/ABSs offered to it by the Serving BS/ABS for handover.

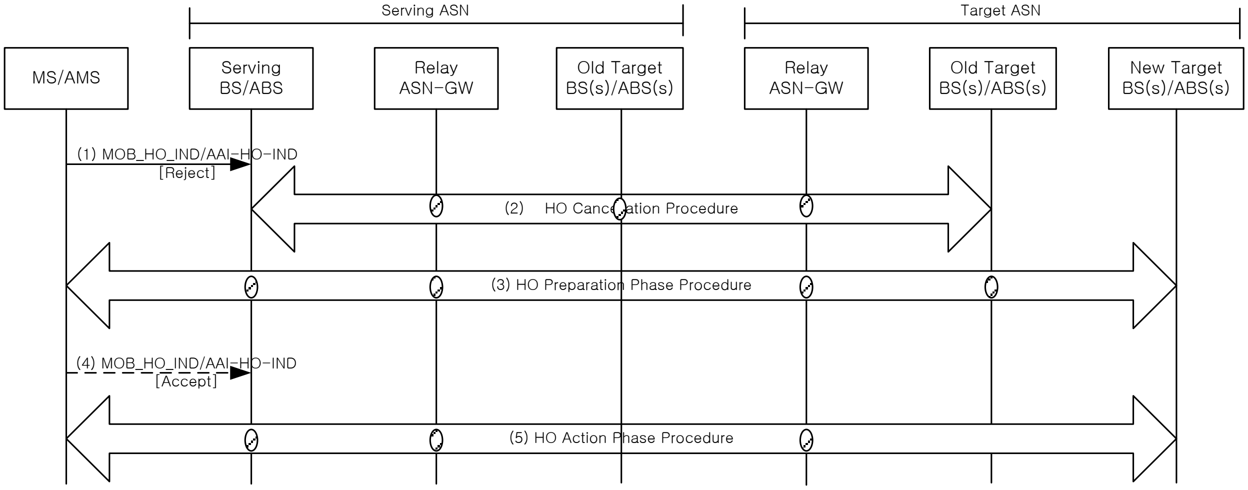

Serving ASN
Target ASN
MS/AMS
Serving BS/ABS
Relay ASN-GW
Old Target BS(s)/ABS(s)
Relay ASN-GW
Old Target BS(s)/ABS(s)
New Target BS(s)/ABS(s)
(1) MOB_HO_IND/AAI-HO-IND [Reject]
(2) HO Cancelation Procedure
(3) HO Preparation Phase Procedure
(4) MOB_HO_IND/AAI-HO-IND [Accept]
(5) HO Action Phase Procedure

Figure 4-100 – MS Handover Rejection

STEP 1

The MS/AMS sends a MOB_HO-IND containing HO_IND_Type TLV set to 0b10 indicating rejection of the target BS/ABS(s) offered by the serving BS/ABS for handover in the MOB_BSHO-RSP (MS initiated handover) or MOB_BSHO-REQ (network initiated handover) message.

[15] The handover rejection procedure described in this section is applicable only to handovers occurring between two Legacy BSs or handovers from a Legacy BS to an Advanced BS. For other handovers cases, rejection of handovers by MS/AMS are not supported.

STEP 2

The Serving BS/ABS initiates the handover cancellation procedures described in section 4.7.2.3 with the Target BS/ABS(s) controlling the Target BS/ABS(s) which were rejected for handover by the MS/AMS.

The following steps only occur if the Serving BS/ABS is able to offer an alternate Target BS/ABS(s) to the MS.

STEP 3

The Serving BS/ABS starts network initiated HO described in 4.7.2.1.5 and initiates the handover preparation procedures with a Target BS/ABS(s) to be offered to the MS/AMS for handover.

STEP 4

The MS/AMS indicates acceptance of a new Target BS/ABS offered by the Serving BS/ABS to the MS/AMS 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/ABS completes the handover action procedures described in section 4.7.2.2 and the MS/AMS completes successful handover to the new Target BS/ABS.

Note: If the MS/AMS rejects the Target BS/ABS offered by the Serving BS/ABS as described in step 1, steps 1-2 are repeated. If the Serving BS/ABS decides to offer a new Target BS/ABS for handover to the MS/AMS, 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/ABS or Anchor ASN-GW to initiate establishment or provide confirmation of the data paths for an MS/AMS, 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, Target ASN-GW or BS/ABS upon sending the R6 *Path_Reg_Rsp* message if no data path has been pre-established for the MS/AMS, and is stopped upon receiving a corresponding R6 *Path_Reg_Ack* message.
- $T_{R6\_Path\_Dereg\_Req}$: is started by the Anchor ASN-GW, BS/ABS or (old) Serving ASN-GW after completion of the Data Path Registration procedure for an MS/AMS, upon sending the R6 *Path_Dereg_Req* message, and is stopped upon receiving a corresponding R6 *Path_Dereg_Rsp* message.
- $T_{R6\_Path\_Dereg\_Rsp}$: is started by the Anchor ASN-GW, BS/ABS or (old) Serving ASN-GW after completion of the Data Path Registration procedure for an MS/AMS, upon sending the R6 *Path_Dereg_Rsp* message, and is stopped upon receiving a corresponding R6 *Path_Dereg_Ack* message
- $T_{R6\_CMAC\_Key\_Count\_Upd}$: is started by a Target (now new Serving) BS/ABS after MS/AMS completes network re-entry, upon sending the R6 *CMAC_Key_Count_Update* message to the Authenticator ASN-GW, and is stopped upon receiving a corresponding R6 *CMAC_Key_Count_Update_Ack* message from the Authenticator ASN-GW.
- $T_{R6\_HO\_Cnf}$: is started by the Serving BS/ABS when sending a R6 *HO_Cnf* message to a Target BS/ABS, and is stopped upon receiving a R6 *HO_Ack* message from the corresponding Target BS/ABS.

- $T_{\text{R6\_HO\_Comp}}$: is started by the Target (now new Serving) BS/ABS after MS/AMS completes network re-entry, upon sending the R6 *HO_Complete* message to the Serving BS/ABS, and is stopped upon receiving a corresponding R6 *HO_Ack* message from the Serving BS/ABS.

This section identifies the timer entities participating in the HO Action Phase. The following timers are defined over R4:

- $T_{\text{R4\_Path\_Reg\_Req}}$: is started by the Target ASN-GW to initiate establishment or provide confirmation of the data paths for an MS/AMS, upon sending the R4 *Path_Reg_Req* message, and is stopped upon receiving a corresponding R4 *Path_Reg_Rsp* message.
- $T_{\text{R4\_Path\_Reg\_Rsp}}$: is started by the Anchor ASN-GW upon sending the R4 *Path_Reg_Rsp* message if no data path has been pre-established for the MS/AMS, and is stopped upon receiving a corresponding R4 *Path_Reg_Ack* message.
- $T_{\text{R4\_Path\_Dereg\_Req}}$: is started by the Anchor ASN-GW or (old) Serving ASN-GW after completion of the Data Path Registration procedure for an MS/AMS, upon sending the R4 *Path_Dereg_Req* message, and is stopped upon receiving a corresponding R4 *Path_Dereg_Rsp* message.
- • $T_{\text{R4\_Path\_Dereg\_Rsp}}$: is started by the Anchor ASN-GW or (old) Serving ASN-GW after completion of the Data Path Registration procedure for an MS/AMS, upon sending the R4 *Path_Dereg_Rsp* message, and is stopped upon receiving a corresponding R4 *Path_Dereg_Ack* message
- $T_{\text{R4\_CMAC\_Key\_Count\_Upd}}$: is started by a Target (now new Serving) ASN-GW after MS/AMS completes network re-entry, upon sending the R4 *CMAC_Key_Count_Update* message to the Authenticator ASN-GW, and is stopped upon receiving a corresponding R4 *CMAC_Key_Count_Update_Ack* message from the Authenticator ASN-GW.
- $T_{\text{R4\_HO\_Comp}}$: is started by the Target (now new Serving) ASN-GW after MS/AMS completes network re-entry, upon sending the R4 *HO_Complete* message to the Serving ASN-GW, and is stopped upon receiving a corresponding R4 *HO_Ack* message from the Serving ASN-GW.

Table 4-84 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 4-84 – HO Action Phase R4 and R6 Timer Values

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{\text{R6\_Path\_Reg\_Req}}$	TBD		TBD
$T_{\text{R6\_Path\_Reg\_Rsp}}$	TBD		TBD
$T_{\text{R6\_Path\_Dereg\_Req}}$	TBD		TBD
$T_{\text{R6\_Path\_Dereg\_Rsp}}$	TBD		TBD
$T_{\text{R6\_CMAC\_Key\_Count\_Upd}}$	TBD		TBD
$T_{\text{R6\_HO\_Cnf}}$	TBD		TBD
$T_{\text{R6\_HO\_Comp}}$	TBD		TBD
$T_{\text{R4\_Path\_Reg\_Req}}$	TBD		TBD
$T_{\text{R4\_Path\_Reg\_Rsp}}$	TBD		TBD
$T_{\text{R4-Path\_Dereg\_Req}}$	TBD		TBD
$T_{\text{R4-Path\_Dereg\_Rsp}}$	TBD		TBD
$T_{\text{R4\_CMAC\_Key\_Count\_Upd}}$	TBD		TBD
$T_{\text{R4 HO Comp}}$	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 4-85 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 4-85.

Table 4-85 – Actions after Timer MAX Retry

Timer	Entity where Timer Started	Action(s)
$T_{R6\_Path\_Reg\_Req}$	Target BS/ABS	BS/ABS shall force MS/AMS to perform initial network entry.
$T_{R6\_Path\_Reg\_Rsp}$	Anchor ASN-GW, Target ASN-GW	ASN-GW shall defer sending the downlink packets until it receives any packets for MS/AMS from Target(new Serving) BS/ABS. ASN-GW shall reset data paths for MS/AMS if no packets are received until a pre-specified system timer expires.
$T_{R6\_Path\_Dereg\_Req}$	Anchor ASN-GW, BS/ABS or (old) Serving ASN-GW	No action required.
$T_{R6\_Path\_Dereg\_Rsp}$	Anchor ASN-GW, BS/ABS or (old) Serving ASN-GW	No action required.
$T_{R6\_CMAC\_Key\_Count\_Upd}$	Target (new Serving) BS/ABS	BS/ABS shall force MS/AMS to perform initial network entry.
$T_{R6\_HO\_Cnf}$	(old) Serving BS/ABS	No action required.
$T_{R6\_HO\_Comp}$	Target BS/ABS	No action required.
$T_{R4\_Path\_Reg\_Req}$	Target ASN-GW	ASN-GW SHALL force MS/AMS to perform initial network entry.
$T_{R4\_Path\_Reg\_Rsp}$	Anchor ASN-GW	ASN-GW SHALL defer sending the downlink packets until it receives any packets for MS/AMS from Target (new Serving) ASN-GW. ASN-GW SHALL reset data paths for MS/AMS if no packets are received until a pre-specified system timer expires.
$T_{R4\_Path\_Dereg\_Req}$	Anchor ASN-GW or (old) Serving ASN-GW	No action required.
$T_{R4\_Path\_Dereg\_Rsp}$	Anchor ASN-GW or (old) Serving ASN-GW	No action required.
$T_{R4\_CMAC\_Key\_Count\_Upd}$	Target (new Serving) ASN-GW	ASN-GW SHALL force MS/AMS to perform initial network entry.
$T_{R4\_HO\_Comp}$	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/ABS /ASN-GW SHALL stop $T_{R6\_Path\_Reg-Req}$/$T_{R4\_Path\_Reg-Req}$ (if running). The Target BS/ABS/ASN-GW MAY re-send the *Path_Reg_Req* message. If the Target BS/ABS/ASN-GW does not resend the *Path_Reg_Req* message or if subsequent attempts are also unsuccessful, the Target BS/ABS SHALL force the MS/AMS to perform a full network re-entry.

4.7.2.6.3 HO_Cnf Error

If the timer $T_{R6\_HO\_Cnf}$ expires, the Serving BS/ABS may re-send the *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS/ABS stops resending the *HO_Cnf*. The Target BS/ABS SHALL perform the local clean up if *HO_Cnf* is never received from the Serving BS/ABS.

4.7.3 Uncontrolled (Unpredictive) HO with Context Retrieval

An Uncontrolled (Unpredictive) handover occurs when an MS/AMS starts ranging at a Target BS/ABS that wasn't previously notified of an impending handover from an MS/AMS and didn't participate in the Handover Preparation Phase. This may occur due to suboptimal radio planning conditions or MS/AMS implementation (handover notification to the network by the BS/ABS is optional).

If an MS/AMS starts ranging with a BS/ABS that doesn't have MS Context information including Authenticator ASN-GW and Anchor ASN-GW identifiers, the RNG-REQ/AAI-RNG-REQ message from the MS/AMS 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/AMS includes the Serving BS/ABS ID TLV in the RNG-REQ/AAI-RNG-REQ message, the handover can still be completed and the period of traffic unavailability can be greatly reduced. When an MS/AMS re-enters at a Target BS/ABS and supplies its Serving BS/ABS ID in the RNG-REQ/AAI-RNG-REQ message, the Target BS/ABS may retrieve the relevant MS Context from the Serving BS/ABS 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/AMS to authenticate the RNG-REQ/AAI-RNG-REQ and perform data path registration with the Anchor DP ASN-GW. This call flow scenario is described in Figure 4-101.

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/AMS and the data path registration occurs with the Serving ASN-GW. The content of the messages are described in sections 4.7.6.1 and 4.7.6.2. 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/ABS 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)[16]. The moment of Network Re-Entry completion does not affect interoperability and is left as a vendor implementation option.

[16] 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/AMS.

4.7.3.1 Successful Uncontrolled Handover

The following call flow provides an example of a successful uncontrolled handover scenario. A MS/AMS begins ranging at Target BS/ABS that wasn't contacted by the Serving BS/ABS to participate in the Handover Preparation phase. Therefore the Target BS/ABS was unaware of an impending hand-in from the MS/AMS. The MS/AMS includes the Serving BS/ABS ID in the RNG-REQ/AAI-RNG-REQ message. The Target BS/ABS retrieves the MS/AMS context and the Authenticator information and successfully completes the handover.

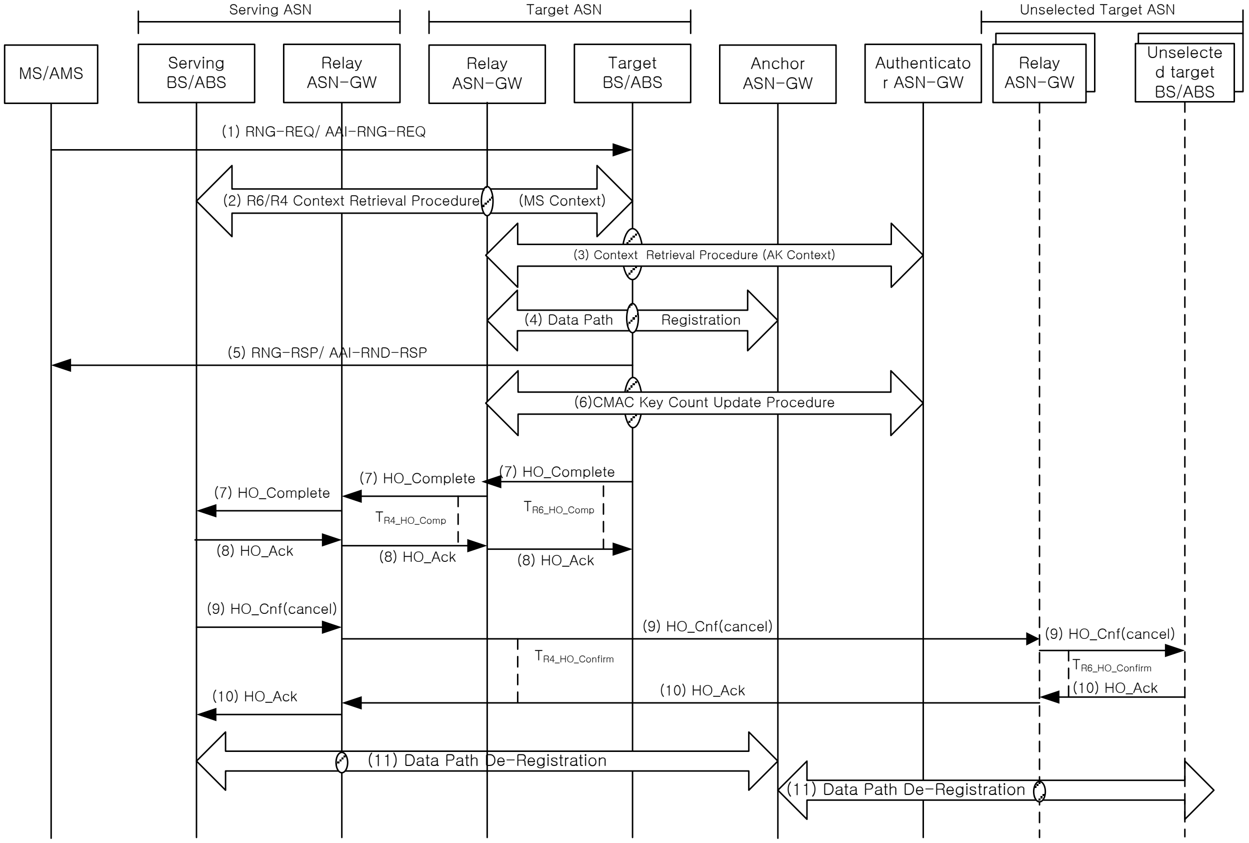


Figure 4-101 – Uncontrolled (Unpredictive) HO

STEP 1

An MS/AMS performs an uncontrolled handover by sending a RNG-REQ/AAI-RNG-REQ message to perform contention based ranging at a Target BS/ABS that didn't receive prior notification of an impending handover from the MS/AMS and therefore didn't participate in the Handover Action/Preparation phase. The MS/AMS includes the Serving BS/ABSID TLV in the RNG-REQ/AAI-RNG-REQ message.

STEP 2

The Target BS/ABS initiates a Context Retrieval procedure with the Serving BS/ABS to retrieve context information for the MS. See section 4.12 for this procedure. The Serving BS/ABS responds by sending the context information which includes the Anchor Authenticator ID and Anchor ASN-GW ID. Optionally, if the Target BS/ABS 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/ABS. 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/ABS supports mobility restriction for stationary access, if the target BS/ABS does not belong to the Reattachment zone, then the target BS/ABS directs the MS to start an initial network entry.

STEP 3

The Target BS/ABS requests AK context for the MS/AMS by initiating a Context Retrieval 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/ABS initiates a Context Retrieval procedure with the Authenticator ASN-GW.

If the MS' mobility access classifier is fixed or nomadic, the MS/AMS' Authenticator will reject AK context requests from the unauthorized Target BS/ABSs based on Authenticator's knowledge of MS Reattachment Zone list. To reject the AK context request from the Target BS/ABS, the MS/AMS' Authenticator responds with Context-Rpt message that includes appropriate Failure Indication value and excludes MS' AK context.

In this case the Target BS/ABS will direct the MS/AMS to start an initial network entry.

STEP 4

The Target BS/ABS initiates data path registration for the MS/AMS 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/ABS, the Serving ASN-GW hosts the Anchor data path function and the Target BS/ABS initiates Data Path Registration procedure (see section 4.12) for the MS/AMS with the Anchor ASN-GW.

STEP 5

Target BS/ABS uses the Authenticator context to authenticate the MS/AMS message. The Target BS/ABS sends a RNG-RSP/AAI-RNG-RSP message to the MS/AMS acknowledging the HMAC/CMAC tuple (expedited security authentication) and containing the *HO Process Optimization/Reentry Process Optimization TLV*.

STEP 6

The Target BS/ABS 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/ABS SHALL send a *HO_Complete* message to the Serving BS/ABS 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/ABS SHALL release the MS context and starts timer $T_{R6\_HO\_Comp}$.

STEP 8

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS. 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/ABS stops timer $T_{R6\_HO\_Comp}$.

STEP 9

The Serving BS/ABS may have already sent the *HO_Cnf* message with the HO_Indication type set to "Cancel" to some or all Target BS/ABSs. For all unselected Target BS/ABSs to which such message has not been sent yet, the Serving BS/ABS SHALL send such a message upon receipt of *HO_Complete* message in order to clear the MS context at Target BS/ABSs. Relay ASN-GW relays the message over R4/R6. When Serving BS/ABS sends *HO_Cnf* message it starts timer $T_{R6\_HO\_Conf.}$

STEP 10

The unselected Target BS/ABS sends a *HO_Ack* message to the Serving BS/ABS. Relay ASN-GW relays the message over R4/R6. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Conf}$.

STEP 11

Upon receiving the *HO_Complete* message, if the Serving BS/ABS still has a data path with Anchor ASN-GW, the Serving BS/ABS SHALL initiate a Data Path De-Registration procedure with the Anchor ASN-GW. See section 4.1.5 for this procedure. Upon completing the Data Path Registration procedure with the Target BS/ABS, the Anchor ASN-GW MAY initiate Data Path De-Registration procedure with the old Serving BS/ABS. 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 BS/ABSs.

4.7.4 Handover between Release 1 and Release 2 Air Interface

4.7.4.1 Handover from Legacy BS to Advanced BS

4.7.4.1.1 Handover to MZone of Advanced BS

During the AMS re-entry at the MZone of the ABS, the MS context information for 802.16m air link connections is re-negotiated between the AMS and the MZone of the ABS.

When the AMS performs handovers from a legacy BS to the MZone of an advanced BS (ABS), the following two procedures shall be used. The first procedure is for Anchor Authenticator that supports Rel 1.0 in the section 4.7.4.1.1.1 and the second for Anchor Authenticator that supportsRelease 2 in the section 4.7.4.1.1.2.

4.7.4.1.1.1 Handover to MZone of Advanced BS when Anchor Authenticator supports Rel 1.0 only

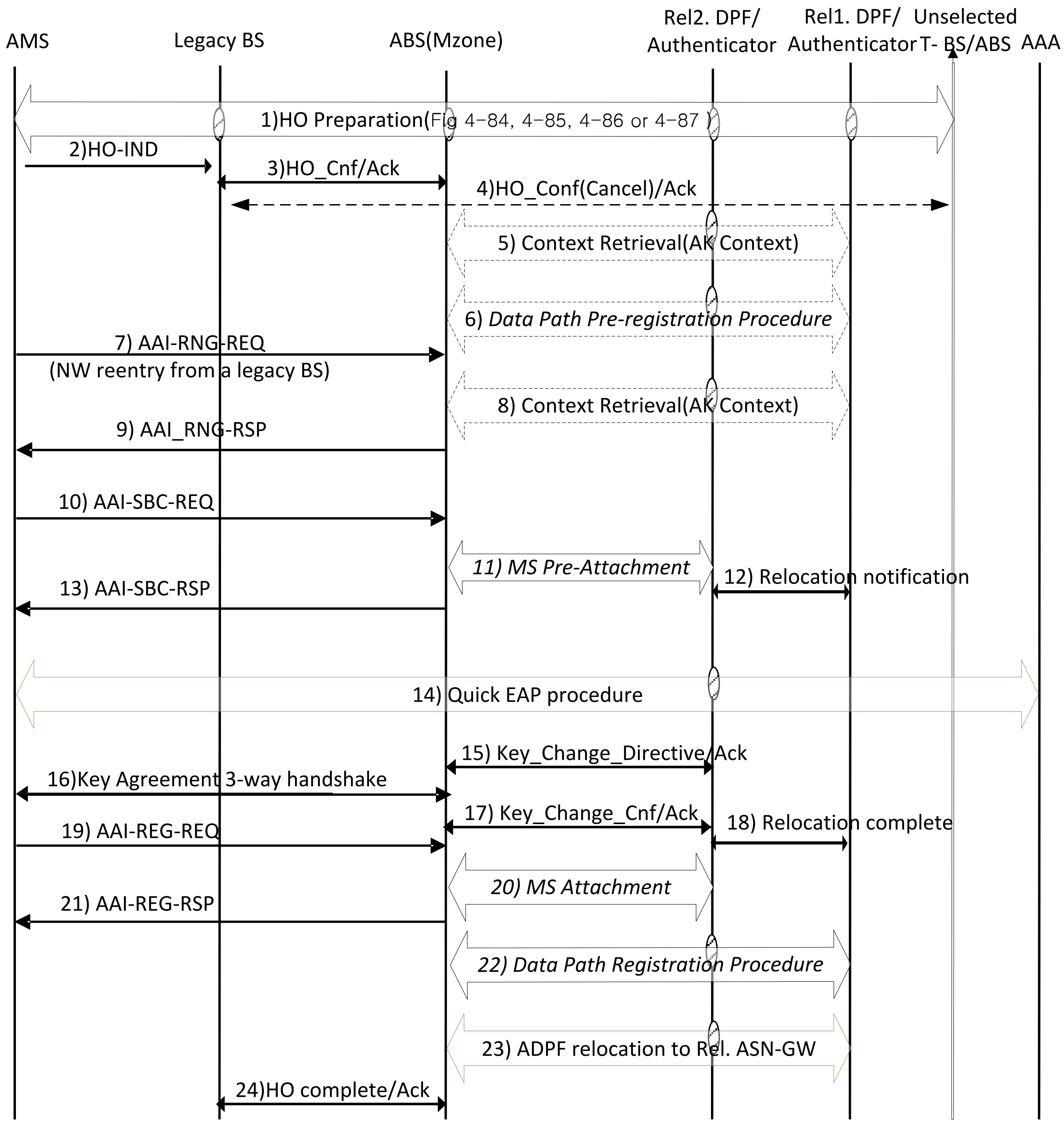


Figure 4-102 – Handover from Legacy BS to Advanced BS (MZone) when the AA supports Rel.1.0

STEP 1

The AMS discovers an ABS(MZone) and decides to directly handover to the ABS(MZone). The AMS sends an MOB-MSHO-REQ message containing the target ABS ID and HO preparation procedure is performed. The details are similar to the procedure described in sections 4.7.2.1.1, 4.7.2.1.2, 4.7.2.1.3 or 4.7.2.1.4 (Figure 4-86, Figure 4-87, Figure 4-88 or Figure 4-89 respectively), which detail the MS initiated HO properation procedure.

This STEP is omitted if the procedure is not a controlled Handover.

STEP 2

The AMS sends a HO-IND message to the serving BS. This STEP is omitted if the procedure is not a controlled Handover.

STEP 3

The serving BS initiates a HO confirm procedure with the Target ABS.

STEP 4

Initiated by the serving BS, the handover cancellation procedure is followed in order to cancel the HO preparation for the other unselected ABS if HO preparation for the other ABS is not cancelled in STEP 3.

This STEP is omitted if it is not a controlled Handover.

STEP 5

The target ABS MAY initiate the Context Retrieval procedure to obtain a new AK context from the Anchor Authenticator if the target ABS didn't obtain a valid AK context yet.

This STEP is omitted if the procedure is not a controlled Handover.

STEP 6

The target ABS MAY initiate the data path pre-registration procedure following the Context Retrieval procedure This STEP is omitted if the procedure is not a controlled Handover.

STEP 7

The AMS sends a CMAC-protected AAI-RNG-REQ message setting its ranging purpose indication as 'Network reentry from a legacy BS' at the target ABS.

STEP 8

The target ABS initiates the Context Retrieval procedure to obtain a new AK context from the Anchor Authenticator if the target ABS didn't obtain a valid AK context yet.

STEP 9

After CMAC validation, the target ABS sends an AAI-RNG-RSP message, which is followed by re-negotiation of MS context information for 802.16m air link connections.

STEP 10

The AMS sends an AAI-SBC-REQ message to the Target ABS to negotiate the 802.16m SBC parameters.

STEP 11

Upon receiving the AAI-SBC-REQ message from the AMS, the Taget ABS initiates MS Pre-Attachement procedure where the MS_Preattachment_Req message contains a L-to-M handover from legacy BS indication TLV to indicate that the AMS is under the L-to-M handover from a legacy BS to the ABS (MZone).

STEP 12

After receiving MS_Preattachment_Req message containing a L-to-M handover from legacy BS indication TLV, the Rel2.x Authenticator initiates re-authentication with AA/ADPF relocation (See section 4.4.1.5.5.2) if anchor ASN-GW is Release 1.x. Steps 9 through 15 are omitted if the anchor Authenticator supports Release 2.0.

STEP 13

The Target ABS responds to the AMS with an AAI-SBC-RSP message which includes the negotiated 802.16m SBC parameters.

STEP 14

In order to expedite EAP authentication a Quick EAP authentication is adopted in place of the EAP authentication (refer to the section 4.4.1.2.4).

STEP 15

The Release 2 Authenticator delivers a new AK context derived from the new MSK by Key_Change_Directive/Ack.

STEP 16

The Key agreement 3-way handshake follows the EAP authentication. Key agreement 3-way handshake messages are integrity protected by the CMAC key based on the new MSK derived during the Step 11.

STEP 17

The ABS indicates the completion of PKMv3 Key agreement 3-way handshake and enforcement of the new keys to the authenticator by Key_Change_Cnf/Ack.

STEP 18

Authenticator Relocation complete procedure follows the reauthentication procedure (i.e. STEP 11 though 14).

STEP 19

The AMS sends an AAI-REG-REQ message to the Target ABS to negotiate 802.16m REG parameters.

STEP 20

Upon receiving the AAI-REG-REQ message from the AMS, the Taget ABS initiates MS Attachement procedure.

STEP 21

The Target ABS responds to the AMS with an AAI-REG-RSP message which includes the negotiated 802.16m REG parameters.

STEP 22

Data path registration procedure follows the registration procedure. Details are shown in section 4.12.3.

STEP 23

ADPF relocation follows the data path registration procedure. Details are shown in section 4.6.5.

STEP 24

The handover procedure is completed by exchanging the HO_Complete messages, which are initiated by the target ABS.

4.7.4.1.1.2 Handover to MZone of Advanced BS when Anchor Authenticator supports Rel 2.0

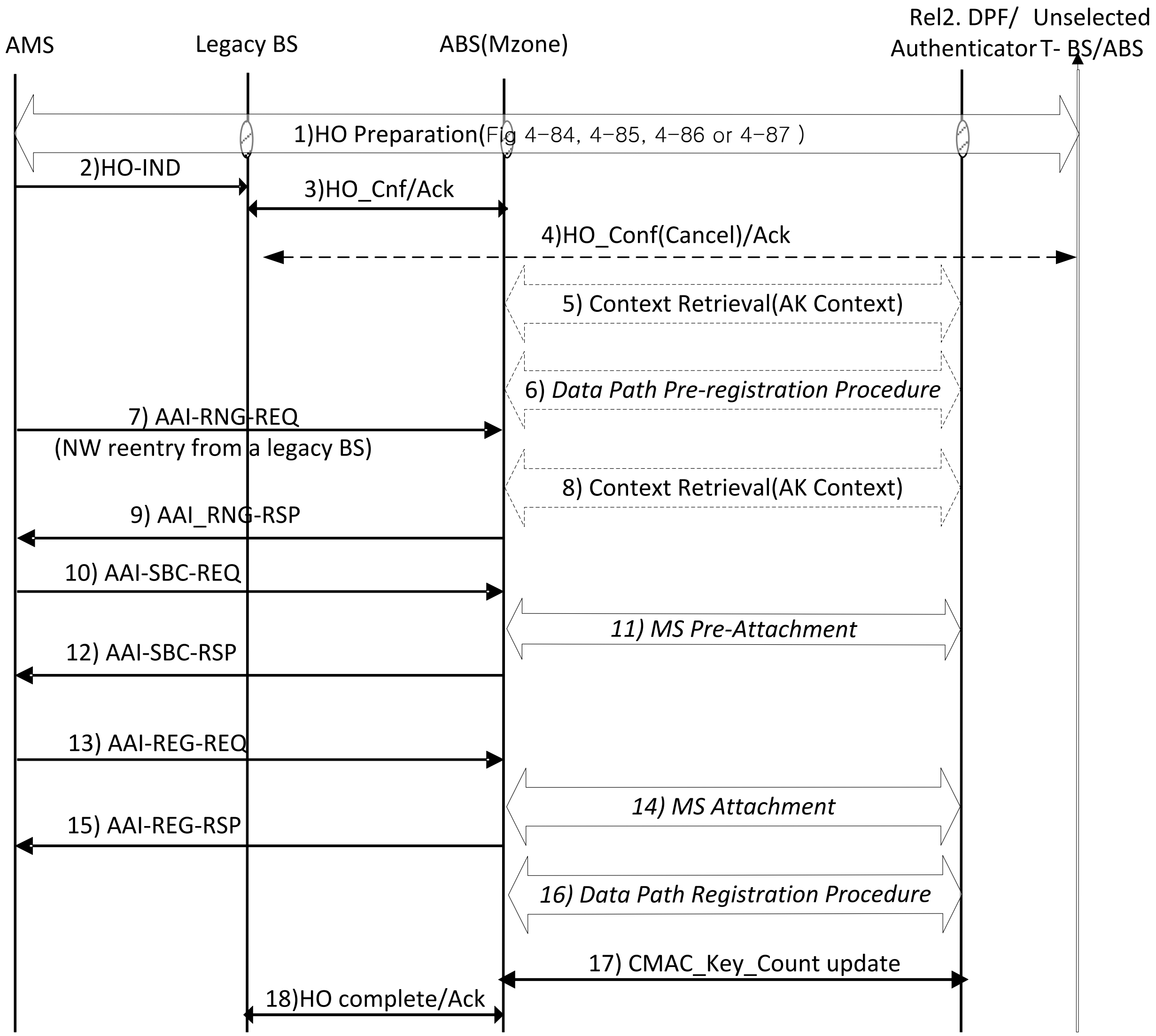


Figure 4-103 – Handover from Legacy BS to Advanced BS (MZone) when the AA supports Rel.2.x

STEP 1

The AMS discovers an ABS(MZone) and decides to directly handover to the ABS(MZone). The AMS sends an MOB-MSHO-REQ message containing the target ABS ID and HO preparation procedure is performed . The details are similar to procedure described in sections 4.7.2.1.1, 4.7.2.1.2, 4.7.2.1.3 or 4.7.2.1.4 (Figure 4-86, Figure 4-87, Figure 4-88 or Figure 4-89 respectively), which detail the MS initiated HO properation procedure.

This STEP is omitted if it is not a controlled Handover.

STEP 2

The AMS sends a HO-IND message to the serving BS. This STEP is omitted if the procedure is not a controlled Handover.

STEP 3

The serving BS initiates a HO confirm procedure with the Target ABS.

STEP 4

Initiated by the serving BS, the handover cancellation procedure is followed in order to cancel the HO preparation for the other unselected ABS if HO preparation for the other ABS is not cancelled in STEP 3.

This STEP is omitted if it is not a controlled Handover.

STEP 5

The target ABS MAY initiate the Context Retrieval procedure to obtain a new AK context from the Anchor Authenticator if the target ABS didn't obtain a valid AK context yet.

This STEP is omitted if the procedure is not a controlled Handover.

STEP 6

The target ABS MAY initiate the data path pre-registration procedure following the Context Retrieval procedure This STEP is omitted if the procedure is not a controlled Handover.

STEP 7

The AMS sends a CMAC-protected AAI-RNG-REQ message setting its ranging purpose indication as 'Network reentry from a legacy BS' at the target ABS.

STEP 8

The target ABS initiates the Context Retrieval procedure to obtain a new AK context from the Anchor Authenticator if the target ABS didn't obtain a valid AK context yet.

STEP 9

After CMAC validation the target ABS sends an AAI-RNG-RSP message, which is followed by re-negotiation of MS context information for 802.16m air link connections..

STEP 10

The AMS sends an AAI-SBC-REQ message to the Target ABS to negotiate 802.16m SBC parameters.

STEP 11

Upon receiving the AAI-SBC-REQ message from the AMS, the Taget ABS initiates MS Pre-Attachement procedure where the MS_Preattachment_Req message contains a L-to-M handover from legacy BS indication TLV to indicate that the AMS is under the L-to-M handover from the legacy BS to the ABS(MZone).

STEP 12

The Target ABS responds to the AMS with an AAI-SBC-RSP message which includes the negotiated 802.16m SBC parameters.

STEP 13

The AMS sends an AAI-REG-REQ message to the Target ABS to negotiate 802.16m REG parameters.

STEP 14

Upon receiving the AAI-REG-REQ message from the AMS, the Taget ABS initiates MS Attachement procedure.

STEP 15

The Target ABS responds to the AMS with an AAI-REG-RSP message, which includes the negotiated 802.16m REG parameters.

STEP 16

Target ABS initiates Data Path Registration procedure (see section 4.12.3) with the Anchor ASN-GW. Note: This procedure is a two-way handshake if data path was pre-established.

STEP 17

Upon successful completion of network re-entry, Target ABS 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 AMS.

STEP 18

The handover procedure is completed by exchanging the HO_Complete messages , which initiated by the target ABS.

4.7.4.1.2 Handover to LZone of Advanced BS

When an AMS performs handover from a legacy BS to the LZone of an advanced BS (ABS), the same handover procedures defined in section 4.7.2 and 4.7.3 shall be used.

4.7.4.2 Handover from Advanced BS to Legacy BS

4.7.4.2.1 Handover from MZone of Advanced BS

When AMS performs handovers from the MZone of an advanced BS (ABS) to a legacy BS, the following call flow shall be used. The MS context information for the 802.16e [11] air link connections shall be re-negotiated during the handover re-entry at the legacy BS.

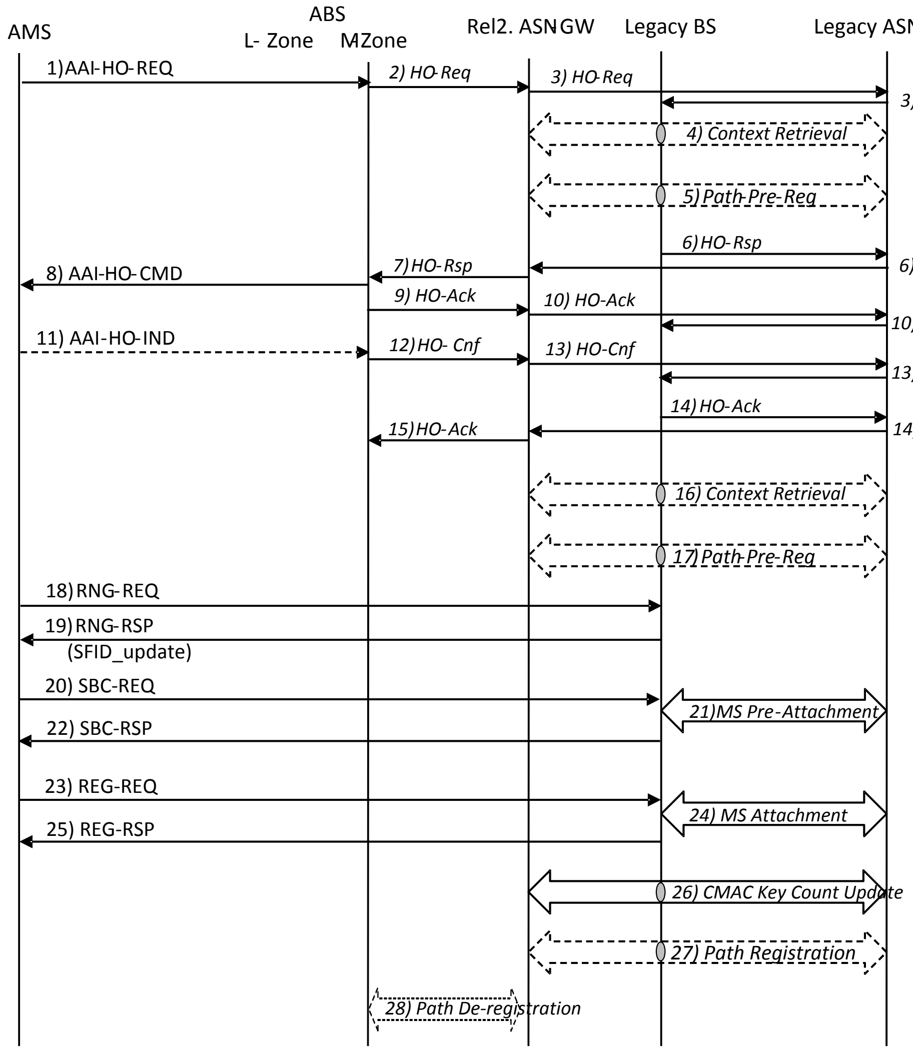


Figure 4-104 – Handover from Advanced BS (MZone) to Legacy BS

STEP 19

The AMS initiates a handover by sending a AAI-HO-REQ message to the Serving ABS which includes one or more candidate Target BS/ABS's.

STEP 20

The Serving ABS sends a *HO_Req* message to each potential Target BS/ABS 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 ABS SHALL silently discard a duplicate AAI-HO-REQ from an MS, if it has already initiated a HO preparation phase for this MS which is still ongoing. If a Serving ABS receives such a duplicate AAI-HO-REQ message from an MS, it SHALL not propagate the request further in to the network.

STEP 21

The Serving Relay ASN-GW sends a *HO_Req* message to the Target BS/ABS and the Serving ASN GW starts timer $T_{R4\ HO\ Req.,}$ If Target Relay ASN-GW involves, it relays the *HO_Req* message to the Target BS/ABS between the Serving Relay ASN-GW and the Target BS/ABS and starts $T_{R/R6\ HO\ Req}$. The Relay ASN-GW may send the message to multiple Target BS/ABS's for the potential handover.

STEP 22

The Target BS(s) requests AK context for the AMS by initiating a Context Retrieval procedure (see section 4.12.2) 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 23

The Target BS(s) may initiate pre-establishment of a data path for the AMS 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 24

The Target BS(s) sends a *HO_Rsp* message to the Serving ABS to acknowledge the handover request where Serving ABS starts timer $T_{R6\_HO\_Rsp}$.

In the case that the 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 25

The Relay ASN-GW relays the *HO_Rsp* messages to the Serving ABS and starts $T_{R4\ HO\ Rsp}$. Upon receipt of the *HO_Rsp* message, the Serving ABS stops timer $T_{R6\_HO\_Req}$.

STEP 26

The Serving ABS sends an AAI-HO-CMD message to the AMS containing one or more potential Target BS/ABS's selected by the network for the AMS to handover.

STEP 27

The Serving ABS sends a *HO_Ack* message to the Target BS/ABS(s).

STEP 28

The Relay ASN-GW relays the *HO_Ack* message(s) to the corresponding Target BS/ABS(s). Upon receipt of the *HO_Ack* message, the Target BS/ABS(s) stops the timer $T_{R6\_HO\_Rsp}$.

STEP 1

The AMS sends an AAI-HO-IND to the Serving ABS to indicate a handover to one of the Target BSs proposed or selected by the Serving ABS in the Handover Preparation phase or potentially to a Target BS which has not been proposed by the Serving ASN-GW/ABS in the Handover Preparation phase. This step is skipped, if the AAI-HO-

CMD message sent during the Preparation phase included a single candidate Target BS and the handover to the Target BS is supported by the AMS.

STEP 29

Upon reception of the AAI-HO-IND the Serving ABS sends a *HO_Cnf* message to the selected Target BS and starts timer $T_{R6\_HO\_Conf}$. The Serving ABS MAY also send *HO_Cnf* message with the value of the HO_Indication Type set to “Cancel” to all unselected Target BS/ABS(s) and clear the MS context anytime after receiving AAI-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/or was not included in the AAI-HO-CMD, the *HO_Cnf* message SHALL also include the Authenticator GW ID or AK context, and Anchor GW ID (Anchor ASN-GW) information.

In the case that the AAI-HO-CMD message sent by the Serving BS included a single candidate Target BS, this step may be started by the Serving ABS right after the Serving ABS sent the AAI-HO-CMD message to the AMS.

STEP 30

Relay ASN-GW relays the *HO_Cnf* message over R6/R4 and starts $T_{R6\ HO\ Cnf}$ /$T_{R4\ HO\ Cnf}$.

STEP 31

The Target BS sends a *HO_Ack* message to the Serving ABS. Upon receipt of the *HO_Ack* message, the Relay ASN GW stops the timer $T_{R6\_HO\_Conf}$/$T_{R4\ HO\ Cnf}$.

STEP 32

Relay ASN-GW relays the *HO_Ack* message over R4/R6. Upon receipt of the *HO_Ack* message, the Serving ABS stops the timer $T_{R6\_HO\_Conf}$.

STEP 33

If an Authenticator ID TLV was included in the *HO_Req* or *HO_Cnf* message and AK context for the AMS was not requested during the Handover Preparation phase, the Target BS requests AK context for the AMS by initiating a Context Retrieval procedure (see section 4.12.2) with the Authenticator ASN-GW.

STEP 34

If the Anchor ASN GW ID TLV was included in the *HO_Req* or *HO_Cnf* message and the 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 35

The AMS initiates network re-entry with the Target BS by sending RNG-REQ.

STEP 36

The Target BS responds with RNG-RSP including SFID_Update TLV.

STEP 37

The AMS sends an SBC-REQ message to the Target BS to re-negotiate 802.16e [11] SBC parameters.

STEP 38

Upon receiving the SBC-REQ message from the AMS, the Target BS initiates MS Pre-Attachment procedure.

STEP 39

The Target BS responds to the AMS with an SBC-RSP message which includes negotiated 802.16e [11] SBC parameters.

STEP 40

The AMS sends an REG-REQ message to the Target BS to re-negotiate 802.16e [11] REG parameters.

STEP 41

Upon receiving the REG-REQ message from the AMS, the Target BS initiates MS Attachment procedure.

STEP 42

The Target BS responds to the AMS with an REG-RSP message which includes negotiated 802.16e [11] REG parameters.

STEP 43

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 the AMS.

STEP 44

The Target BS initiates Data Path Registration procedure (see section 4.12.3) with the Anchor ASN GW.

Note: This procedure SHALL be a two-way handshake if the data path(s) was pre-established. Otherwise, it SHALL be three-way handshake.

STEP 45

The Anchor ASN GW initiates Data Path De-registration procedure (see section 4.12.4) with the Anchor ASN GW, if the data path(s) between the Anchor ASN GW and the old Serving BS has not been released yet.

4.7.4.2.2 Handover from LZone of Advanced BS

When AMS performs handovers from the LZone of an advanced BS (ABS) to the Legacy BS, the same handover procedures as defined in section 4.7.2 and 4.7.3 shall be used.

4.7.4.3 Handover between Different Zones of an ABS

4.7.4.3.1 Zone Switch from LZone to Mzone of an Advanced BS

Zone Switch 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 AMS. When the ASN GW initiates the Zone Switch for an AMS, the following call flows SHALL be used. If the Anchor ASN GW for the AMS is Release1 ASN GW and not capable of Release2 functions, ABS SHALL request the Anchor ASN GW to perform ASN GW Relocation procedure before commanding Zone Switch. The ABS sends an RNG-RSP message with Zone Switch TLV to AMS to command Zone Switch from the LZone to the MZone.

During the AMS re-entry at the MZone of the ABS, MS context information for 802.16m [105] air link connections shall be re-negotiated between the AMS and the ABS.

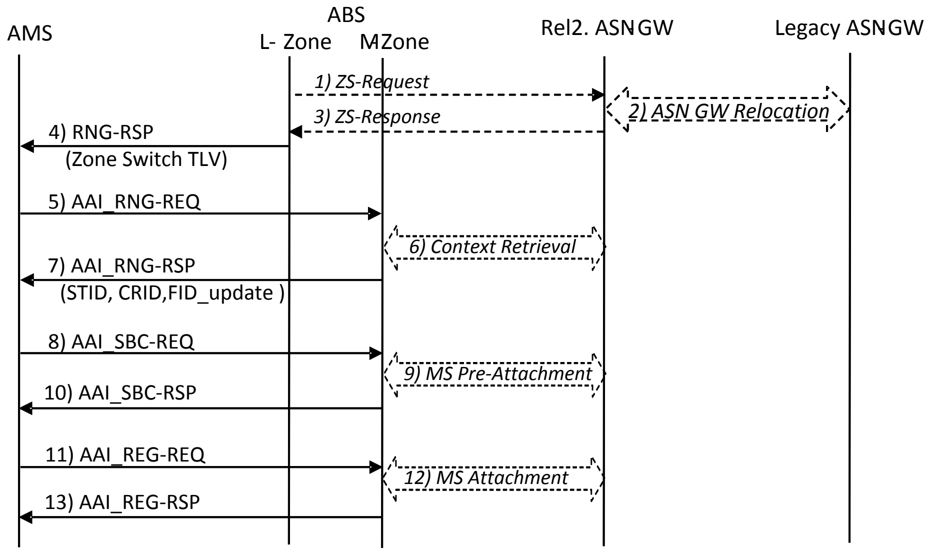


Figure 4-105 – Zone Switch: from LZone to MZone

STEP 1

The ABS sends a *ZS-Request* message to the Serving Relay ASN GW if the zone switch for an AMS is needed. After receiving the *ZS-Request* message, the Serving ASN GW may initiate the Authenticator/Anchor DPF Relocation procedure.

STEP 2

The Serving ASN GW initiates ASN GW Relocation procedure to relocate the Authenticator and the Anchor DPF function.

STEP 3

The Serving ASN GW send a *ZS-Response* message back to the ABS.

STEP 4

The ABS sends the AMS an RNG-RSP message with the “Zone Switch” TLV, to request AMS to perform the Zone Switch.

STEP 5

The AMS sends an AAI-RNG-REQ message at the MZone of the ABS.

STEP 6

The ABS initiates the Context Retrieval procedure to obtain a new AK Key from the Authenticator GW.

STEP 7

The ABS sends AAI-RNG-RSP message to the AMS to acknowledge the network re-entry at the MZone for the Zone Switch.

STEP 8

The AMS sends an AAI-SBC-REQ message to the Target ABS to re-negotiate 802.16m [105] AAI-SBC parameters.

STEP 9

Upon receiving the AAI-SBC-REQ message from the AMS, the Target ABS initiates MS Pre-Attachment procedure.

STEP 10

The Target ABS responds to the AMS with an AAI-SBC-RSP message which includes negotiated 802.16m [105] SBC parameters.

STEP 11

The AMS sends an AAI-REG-REQ message to the Target ABS to re-negotiate 802.16m [105] AAI-REG parameters.

STEP 12

Upon receiving the AAI-REG-REQ message from the AMS, the Target ABS initiates MS Attachment procedure.

STEP 13

The Target ABS responds to the AMS with a AAI-REG-RSP message which includes negotiated 802.16m [105] AAI-REG parameters.

4.7.4.3.2 Zone Switch from MZone to Lzone of an Advanced BS

Zone Switch 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 AMS. When the ASN GW initiated the Zone Switch for an AMS, the following call flows shall be used. The ABS sends the AMS an AAI-HO-CMD message with the HO Type set to 'Zone Switch', to command Zone Switch from the MZone to the LZone.

During the AMS re-entry at the LZone of the ABS, MS context information for 802.16e [11] air link connections shall be re-negotiated between the AMS and the ABS.

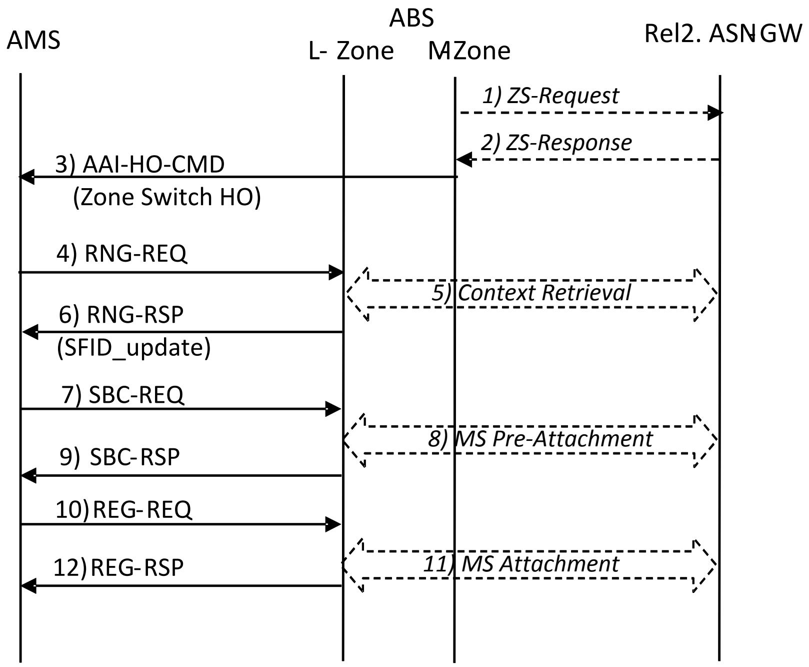


Figure 4-106 – Zone Switch: from MZone to LZone

STEP 1

The ABS sends a *ZS-Request* message to the ASN GW if the zone switch for an AMS is needed.

STEP 2

The ASN-GW sends a *ZS-Response* message to the ABS to acknowledge the zone switch request from the ABS. Or, it may start zone switch procedure by sending a *ZS-Response* message by itself, if the zone switch for an AMS is needed.

STEP 3

The ABS sends the AMS an AAI-HO-CMD message with the HO Type set to the “Zone Switch”, to request AMS to perform the Zone Switch.

STEP 4

The AMS sends a RNG-REQ message at the LZone of the ABS.

STEP 5

The ABS initiates the Context Retrieval procedure to obtain a new AK Key from the Authenticator GW.

STEP 6

The ABS sends an RNG-RSP message to the AMS.

STEP 7

The AMS sends a SBC-REQ message to the Target ABS to re-negotiate 802.16e [11] SBC parameters.

STEP 8

Upon receiving the SBC-REQ message from the AMS, the Target ABS initiates MS Pre-Attachment procedure.

STEP 9

The Target ABS responds to the AMS with a SBC-RSP message which includes negotiated 802.16e [11] SBC parameters.

STEP 10

The AMS sends a REG-REQ message to the Target ABS to re-negotiate 802.16e [11] REG parameters.

STEP 11

Upon receiving the REG-REQ message from the AMS, the Target ABS initiates MS Attachment procedure.

STEP 12

The Target ABS responds to the AMS with a REG-RSP message which includes negotiated 802.16e [11] REG parameters.

4.7.5 HO and Scanning Control for Fixed/Nomadic SS/MS

In [11], Neighbor list of BS/ABSs are advertised through broadcast message, MOB_NBR-ADV/AAI-NBR-ADV, and all MS/AMSs whether Fixed/Nomadic or Full mobility see this message. An MS/AMS, 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/AMS, when it sees the over the air advertised Neighbor list of MS/AMSs, starts scanning like an unrestricted MS/AMS and if the RF conditions are suitable, generates a Handoff request at the current serving BS/ABS, to the new Target BS/ABS. Since a Fixed/Nomadic MS/AMS has restricted mobility, this scanning may generate a lot of spurious handoff requests to non-allowed Target BS/ABSs, 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/AAI-SCN-REQ. A general call flow is given below.

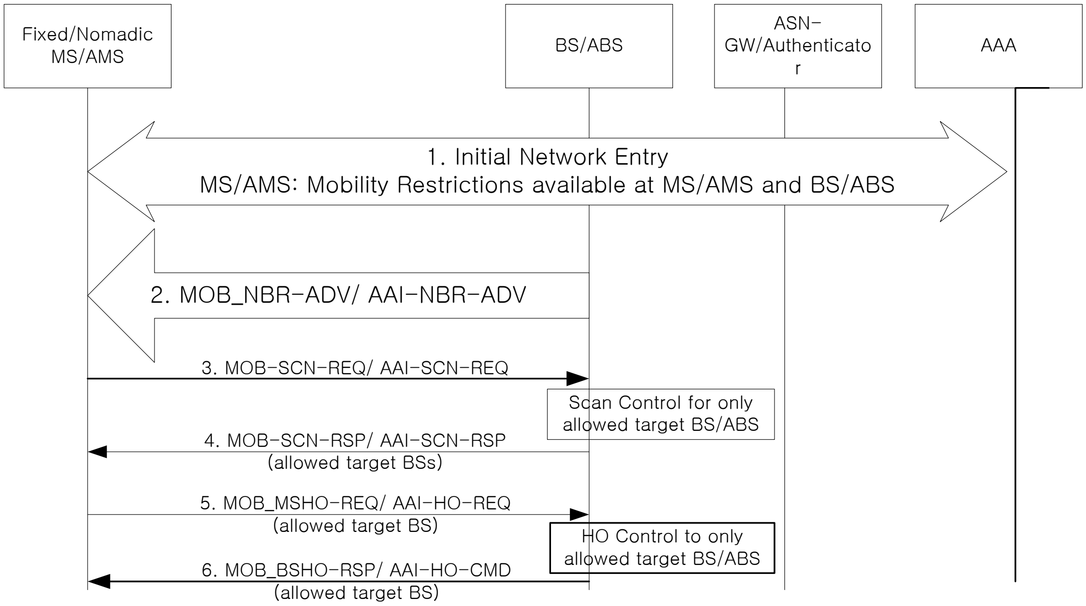

Fixed/Nomadic MS/AMS
BS/ABS
ASN-GW/Authenticator
AAA
1. Initial Network Entry
MS/AMS: Mobility Restrictions available at MS/AMS and BS/ABS
2. MOB_NBR-ADV/ AAI-NBR-ADV
3. MOB-SCN-REQ/ AAI-SCN-REQ
Scan Control for only allowed target BS/ABS
4. MOB-SCN-RSP/ AAI-SCN-RSP
(allowed target BSs)
5. MOB_MSHO-REQ/ AAI-HO-REQ
(allowed target BS)
HO Control to only allowed target BS/ABS
6. MOB_BSHO-RSP/ AAI-HO-CMD
(allowed target BS)

Figure 4-107 – HO and Scanning Control for Fixed/Nomadic SS/MS/AMS

STEP 1

Initial Network Entry as described in section 4.5 and Figure 4-55. SS/MS/AMS's Fixed Nomadic restrictions are known to Authenticator as well as the Serving BS/ABS.

STEP 2

BS/ABS performs default advertisement of its available Target BS/ABSs to all MS/AMSs irrespective of their mobility class.

STEP 3

A Fixed/Nomadic MS/AMS makes request for scanning slots for all Target BS/ABSs in the neighbor advertisement, MOB_NBR-ADV/AAI-NBR-ADV message.

STEP 4

The BS/ABS recognizes the Fixed/Nomadic restriction of the SS/MS/AMS and does scanning control to only allowed Target BS/ABSs 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/AAI-SCN-RSP. In the case of Fixed SS/MS/AMS this list may be zero.

STEP 5

When RF conditions and thresholds are met, the SS/MS/AMS makes handoff request to serving BS/ABS with allowed BSs as its target.

STEP 6

The Serving BS/ABS, receives the handoff request. It checks and performs handoff control based on the mobility restrictions applicable for the particular MS/AMS and sends MOB_BSHO-RSP/AAI-HO-CMD back.

4.7.6 Message Definitions for HO Preparation Phase

4.7.6.1 Message Definitions for HO Preparation Phase

This section describes the R4 message definitions for the HO Preparation Phase.

Table 4-86 – HO_Req

IE	Reference	M/O	Notes	Applicability
HO Type	5.3.2.79	M		1,2,3
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/ABS does not support combining of Data Path Control and HO Control message, it ignores this TLV.	1,2,3
MS Info	5.3.2.103	M		1,2,3
>Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS/AMS. 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/AMS 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.	1,2,3
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1,2,3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1,2,3
>NSP ID	5.3.2.368	O	NSP identifier. Used to help distinguish the R4 and R6 tunnels for a specific NSP.	1,2,3
>Anchor ASN GW ID	5.3.2.10	M	Identifies the node that hosts the Anchor DP Function in the Anchor ASN.	1,2,3
>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.	1,2,3

IE	Reference	M/O	Notes	Applicability
>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.	1,2,3
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.	1,2,3
> Carrier Preassignment Indications	5.3.2.540	O	This TLV May be included when AMS supports MC mode=0b010 or 0b011 or 0b100.	3
>SBC Context	5.3.2.174	O[1]	802.16e/16m related MS session context.	1,2,3
>>HARQ Context (one or more)	5.3.2.453	O	Contains HARQ related information for UL and DL management connections.	1,2,
>>>Direction	5.3.2.59	O	Indicates the direction of the management connection.	1,2,
>>>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.	1,2,
>>>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.	1,2,
>>>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	1,2,
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>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.	1,2
>>PKM Flow Control	5.3.2.319	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>Maximum Number of Supported Security Associations	5.3.2.320	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2,3
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>MAC Mode	5.3.2.322	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>Association type support	5.3.2.465	O		1,2
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O		3
>>DEVICE_CLASS	5.3.2.504	O		3
>>CLC Request	5.3.2.505	O		3
>>Long TTI for DL	5.3.2.506	O		3

IE	Reference	M/O	Notes	Applicability
>>UL sounding	5.3.2.507	O		3
>>OL Region	5.3.2.508	O		3
>>DL resource metric for FFR	5.3.2.509	O		3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O		3
>>DL MIMO mode	5.3.2.512	O		3
>>feedback support for DL	5.3.2.513	O		3
>>Subband assignment A-MAP IE support	5.3.2.514	O		3
>>DL pilot pattern for MU MIMO	5.3.2.515	O		3
>>Number of Tx antenna of AMS	5.3.2.516	O		3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O		3
>>UL pilot pattern for MU MIMO	5.3.2.519	O		3
>>UL MIMO mode	5.3.2.520	O		3
>>Modulation scheme	5.3.2.521	O		3
>>UL HARQ buffering capability	5.3.2.522	O		3
>>DL HARQ buffering capability	5.3.2.523	O		3
>>AMS DL processing capability per sub-frame	5.3.2.524	O		3
>>AMS UL processing capability per sub-frame	5.3.2.525	O		3
>>FFT size(2048/1024/512)	5.3.2.526	O		3
>>Authorization policy support	5.3.2.21	O		3
>>Inter-RAT Operation Mode	5.3.2.527	O		3
>>Supported Inter-RAT type	5.3.2.528	O		3

IE	Reference	M/O	Notes	Applicability
>>MIH Capability Supported	5.3.2.529	O		3
>REG Context	5.3.2.144	O[1]	802.16e related MS session context.	1,2,3
>>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.	1,2
>>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.	1,2
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>DSx Flow Control	5.3.2.294	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>Maximum MAC Data per Frame Support	5.3.2.296	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>>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.	1,2
>>>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.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC ertPS Support	5.3.2.300	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O		3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O		3
>>Multicarrier capabilities	5.3.2.485	O		3
>>Zone Switch Mode Support	5.3.2.486	O		3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O		3
>>Interference mitigation supported	5.3.2.488	O		3
>>E-MBS capabilities	5.3.2.489	O		3
>>Channel BW and Cyclic prefix	5.3.2.490	O		3
>>frame configuration to support legacy R1.0	5.3.2.491	O		3
>>Persistent Allocation support	5.3.2.492	O		3
>>Group Resource Allocation support	5.3.2.493	O		3
>>Co-located coexistence capability support	5.3.2.494	O		3
>>HO Trigger Metric Support	5.3.2.326	O		3
>>EBB Handover support	5.3.2.495	O		3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O		3
>>Capability for sounding antenna switching support	5.3.2.497	O		3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O		3
>>ROHC support	5.3.2.499	O		3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O		3
>SA Descriptor (one or more)	5.3.2.170	O[1]	SHOULD be included by Serving ASN for the Target ASN.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>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/ABS supports Mobility Restriction for stationary access and the MS mobility access classifier is known at the BS/ABS.	1,2,3
>Reattachment Zone	5.3.2.424	O	Indicates the list of BS IDs allowed for reattachment. Included if Mobility Access Classifier is included.	1,2,3
>SF Info (one or more)	5.3.2.185	M		1,2,3
>>SFID	5.3.2.184	M		1,2,3
>>SF Type	5.3.2.306	O		1,2,3
>>Direction	5.3.2.59	M		1,2,3
>>CS Type	5.3.2.39	O	This TLV must be included in the transmitted message for the target ASN to setup flow.	1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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	1,2
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.	1,2,3
>>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.	1,2
>>>ARQ WINDOW SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1,2
>>>ARQ RETRY TIMEOUT-Transmitter Delay	5.3.2.347	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>>ARQ RETRY TIMEOUT-Receiver Delay	5.3.2.348	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ BLOCK LIFETIME	5.3.2.349	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ SYNC LOSS TIMEOUT	5.3.2.350	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ DELIVER IN ORDER	5.3.2.351	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ RX PURGE TIMEOUT	5.3.2.352	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ BLOCK SIZE	5.3.2.353	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>RECEIVER ARQ ACK PROCESSING TIME.	5.3.2.354	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>SN Feedback Enabled field	5.3.2.468	O		1,2
>>FSN Size	5.3.2.469	O		1,2
>>CID	5.3.2.29	O		1,2
>>SAID	5.3.2.169	O		1,2,3
>>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/ABS does not support combining of Data Path Control and HO Control message, it ignores this TLV as well as its child TLV(s).	1,2,3
>>>Data Path ID	5.3.2.44	O	This TLV SHALL be included if Data Path Info is included in the transmitted message.	1,2,3
>>>Tunnel Endpoint	5.3.2.194	O		1,2,3
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	The TLV SHALL be included for active service flows. This parameter is optional for the service flows that are not already activated.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>>Classification Rule Index	5.3.2.30	M	Index assigned to the Packet Classification Rule.	1,2,3
>>> Classification Rule Priority	5.3.2.32	M		1,2,3
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, …	1,2,3
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.	1,2,3
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.	1,2,3
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.	1,2,3
>>>IPv6 Flow Label	5.3.2.470	O		1,2,3
>>QoS Parameters	5.3.2.141	M		1,2,3
>>> DSCP	5.3.2.409	O	TC bit set to 1	1,2,3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>> 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.	1,2,3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1,2,3
>>>>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.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1,2,3
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1,2,3
>>>Media Flow Type	5.3.2.94	O		1,2,3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1,2,3
>>>Reduced Resources Code	5.3.2.237	O		1,2,3
>>PHS Rule	5.3.2.127	O		1,2,3
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSF	0	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
BS Info (Serving)	5.3.2.26	M		1,2,3

IE	Reference	M/O	Notes	Applicability
>BS ID	5.3.2.25	M		1,2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.	1,2,3
>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.	1,2,3
>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.	1,2,3
>UL PHY Quality Info	5.3.2.197	O	MAY be included in order to allow the Target ASN to estimate whether the MS can receive the same quality of service as in the Serving ASN.	1,2,3
> 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.	1,2,3
BS Info (Target, one or more)	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M		1,2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1,2,3
>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/ABS does not support combining of AK Context and HO Control message, it ignores this TLV as well as its child TLV(s).	1,2,3
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>Relative Delay	5.3.2.146	O	MAY be included in order to allow the Target BS/ABS to estimate whether the MS can receive the same quality of service as in the Serving ASN.	1,2,3
>DL PHY Quality Info	5.3.2.60	O	MAY be included in order to allow the Target BS/ABS to estimate whether the MS can receive the same quality of service as in the Serving BS/ABS.	1,2,3
>UL PHY Quality Info	5.3.2.197	O	MAY be included in order to allow the Target ASN to estimate whether the MS can receive the same quality of service as in the Serving ASN.	1,2,3
Certified-MS-Feature-List-For-GW	5.3.2.171	O[2]	List of MS Certified features for the GW.	1,2,3
Certified-MS-Feature-List-For-BS	5.3.2.183	O[3]	List of MS Certified features for the BS/ABS.	1,2,3

Note [1] : This TLV SHALL be included either in HO_Req or in HO_Cnf message.

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.

The Context_Req that is sent from the Target ASN to the Authenticator ASN is shown on the Table 4-87.

Table 4-87 – Context_Req from Target BS/ABS to Authenticator ASN-GW

IE	Reference	M/O	Notes	Applicability
Context Purpose Indicator	5.3.2.36	M	Set to indicate retrieval of AK Context.	1.2.3
MS Info	5.3.2.103	M		1.2.3
>Authenticator ID	5.3.2.19	M		1.2.3
BS Info (Serving)	5.3.2.26	M	Included in order to allow the Authenticator to apply authorization policies depending on Serving BS/ABS.	1.2.3
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.	1.2.3
>BS ID	5.3.2.25	M		1.2.3
BS Info (Target) (one or more)*	5.3.2.26	M		1.2.3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2.3
>BS ID	5.3.2.25	M		1.2.3

The *Context_Rpt* sent from the Authenticator GW to the Target GW appears as shown on the Table 4-88:

Table 4-88 – Context_Rpt from Authenticator ASN-GW to Target BS/ABS

IE	Description	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Request Success or request failure or partial response.	1.2.3
Context Purpose Indicator	5.3.2.36	M	Set to indicate that that the Report contains AK Context.	1.2.3
MS Info	5.3.2.103	O		1.2.3
>Service Authorization Code	5.3.2.181	O	May be included to convey Authorization Policy to the Target BS/ABS.	1.2.3
BS Info (Target)	5.3.2.26	M	Note 1.	1.2.3
>BS ID	5.3.2.25	M		1.2.3
> AK Context	5.3.2.6	M		1.2.3
>>AK	5.3.2.5	M		1.2.3
>>AK ID	5.3.2.7	M		1.2.3
>>AK Lifetime	5.3.2.8	M		1.2.3
>>AK SN	5.3.2.9	M		1.2.3
>>CMAC_KEY_COUNT	5.3.2.34	M		1.2.3
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).	1.2.3

Note 1:. In both R6 and R4 handover messages, as well as on R8 handover message, only one target BS/ABS Info is contained.

Note 2: If the Authenticator ASN-GW supports context retrieval procedure only for 1 BS/ABS at a time, then it includes the context information for the first BS/ABS 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 BS/ABSs and not all BS/ABSs requested in the message, the Authenticator ASN-GW includes the context information for the BS/ABSs 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 4-89.

1 **Table 4-89 – HO_Rsp**

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1.2.3
HO Type	5.3.2.79	M		1.2.3
MS Info	5.3.2.103	M		1.2.3
>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 *HO_Req* or b) the Target ASN needs to deliver per-SF Data Path Info.	1.2.3
>>SFID	5.3.2.184	M		1.2.3
>> Reservation Result	5.3.2.152	M		1.2.3
>>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/ABS does not support combining of Data Path Control and HO Control message, it ignores this TLV as well as its child TLV(s).	1.2.3
>>>Data Path ID	5.3.2.44	O	This TLV SHALL be included if Data Path Info is included in the transmitted message.	1.2.3
>>>Tunnel Endpoint	5.3.2.194	O		1.2.3
BS Info (Serving)	5.3.2.26	M	It MAY be included in order to facilitate message delivery in the presence of HO Relay.	1.2.3
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.	1.2.3
>BS ID	5.3.2.25	M		1.2.3
BS Info (Target)	5.3.2.26	M	Note 1.	1.2.3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2.3
>BS ID	5.3.2.25	M		1.2.3

IE	Reference	M/O	Notes	Applicability
>BS HO RSP Code	5.3.2.203	O	0: VOID 1: Target BS/ABS doesn't support this HO Type; 2: Target BS/ABS rejects for other reasons; 3: Target BS/ABS's CPU overload; 4: Target BS/ABS rejects for other reasons; 5-255: Reserved. This TLV SHALL be mandatory if multiple target BS/ABS Info TLVs are present and if one of the Target BS/ABS handover transaction. If only one Target BS/ABS 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.	1.2.3
>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/ABS (within the Target ASN) during HO. If included, its value has to be delivered to the MS with MOB_BSHO-REQ/AAI-HO-CMD or MOB_BSHO-RSP/AAI-HO-CMD.	1.2
>STID	5.3.2.473	O	MAY be included if an STID is assigned to the MS for use in initial ranging to the Target BS/ABS (within the Target ASN) during HO. If included, its value has to be delivered to the MS with AAI-HO-CMD.	3
>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/AAI-HO-CMD or MOB_BSHO-RSP/AAI-HO-CMD.	1.2.3
>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/AAI-HO-CMD or MOB_BSHO-RSP/AAI-HO-CMD.	1.2.3
> HO Authorization Policy Support	5.3.2.367	O	The value has to be delivered to the MS with MOB_BSHO-RSP/AAI-HO-CMD.	1.2.3

IE	Reference	M/O	Notes	Applicability
>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/AAI-HO-CMD or MOB_BSHO-RSP/AAI-HO-CMD. This value is defined in absolute number of airframes.	1.2.3
> Time Stamp	5.3.2.358	O	HO Response transmission time from the Target BS/ABS. MAY be included in order to allow the Serving ASN to estimate the message propagation delay.	1.2.3
> 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.	1.2.3
> Carrier Status Indication	5.3.2.541	O	Indicating whether this pre-assigned carrier will be activated immediately after HO procedure is done. Shall be included when one or more carriers of the AMS is pre-assigned by the T-ABS.	3
> Physical carrier index of the secondary carrier index	5.3.2.542	O	Physical carrier index of the preassigned secondary carrier, which is pair with the Carrier Status Indication TLV. Shall be included when one or more carriers of the AMS is pre-assigned by the T-ABS.	3
> PHY Carrier Index	5.3.2.543	O	Physical carrier index of the recommended T-ABS. This TLV Shall be included when T-ABS is not included in AAI-NBR-ADV message or is multicarrier ABS.	3
> Ranging Initiation Deadline	5.3.2.544	O	An AMS shall send the AAI-RNG-REQ message during HO until Ranging initiation deadline. This TLV Shall not be included if the target BS is legacy BS.	3
> Pre-assigned MAPMask Key	5.3.2.545	CM	The value of this parameter is the seed used at the T-ABS to initiate the PRBS generator used to scramble the 40-bit A-AMAP IE when the value of the STID included in this message is used as the CRC Mask Masking Code.	3

IE	Reference	M/O	Notes	Applicability
> S-SFH Change Count	5.3.2.546	O	S-SFH change count of the reference for the included SFH delta information. This TLV Shall be included when SFH delta information is included	3
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).	1.2.3

Note 1: In both on R6 and R4 handover messages, as well as on R8 handover message, only one target BS/ABS 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 4-90:

Table 4-90 – HO_Ack

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1.2.3
BS Info (Target)	5.3.2.26	M		1.2.3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2.3
>BS ID	5.3.2.25	M		1.2.3
>Action Time	5.3.2.4	O	Number of frames where the Target BS/ABS 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.	1.2.3
>Time Stamp	5.3.2.358	O	Transmission time for MOB_BSHO-REQ/AAI-HO-CMD or MOB_BSHO-RSP/AAI-HO-CMD 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.	1.2.3

The content of the *Path_Prereg_Req* is specified in the Table 4-91.

1 **Table 4-91 – Path_Prereg_Req**

IE	Reference	M/O	Notes	Applicability
Registration Type	5.3.2.145	M		1.2.3
MS Info	5.3.2.103	M		1.2.3
>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.	1.2.3
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1.2.3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1.2.3
>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.	1.2.3
>SF Info (one or more)	5.3.2.185	M	It SHALL be included if the R4 Tunneling granularity is per SF.	1.2.3
>>SFID	5.3.2.184	M		1.2.3
>>Direction	5.3.2.59	M	Specifies the direction of the reservation.	1.2.3
>>Data Delivery Trigger	5.3.2.265	O	Triggers data delivery for the specified service flow.	1.2.3
>>CID	5.3.2.29	O	It SHALL be included if the Anchor ASN allocates CID.	1.2
>>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.	1.2.3
>>>Data Path ID	5.3.2.44	O		1.2.3
>>>Tunnel Endpoint	5.3.2.194	O		1.2.3
>>QoS Parameters	5.3.2.141	O	It MAY be included on R6 when the target ASN-GW is not the Anchor GW.	1.2.3
BS Info (Target)	5.3.2.26	M		1.2.3

IE	Reference	M/O	Notes	Applicability
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2.3
>BS ID	5.3.2.25	M		1.2.3

The content of *Path_Prereg_Rsp* is shown on the Table 4-92.

Table 4-92 – Path_Prereg_Rsp

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1.2.3
Registration Type	5.3.2.145	M		1.2.3
Result Code	5.3.2.154	O	Result Code TLV SHALL be present in the case of a failure condition Enumerator: The values are: • 0x01 = Failure – No resources • 0x02 = Failure – Not supported	1.2. 1.2.33
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.	1.2.3
>SF Info (one or more)	5.3.2.185	M	It SHALL be included if the R4 Tunneling granularity is per SF.	1.2.3
>>SFID	5.3.2.184	M		1.2.3
>>QoS Parameters	5.3.2.141	O	It MAY be included on R6 when the target ASN-GW is not the Anchor GW.	1.2.3
>>Data Delivery Trigger	5.3.2.265	O	Triggers data delivery for the specified service flow.	1.2.3
>>CID	5.3.2.29	O		1.2
>>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.	1.2.3
>>>Data Path ID	5.3.2.44	O		1.2.3
>>>Tunnel Endpoint	5.3.2.194	O		1.2.3
BS Info (Target)	5.3.2.26	M		1.2.3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2.3
>BS ID	5.3.2.25	M		1.2.3

The content of *Path_Reg_Ack* is shown on the Table 4-93.

Table 4-93 – Path_Prereg_Ack

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1.2.3
Registration Type	5.3.2.145	M		1.2.3

4.7.6.2 Message Definitions for HO Action Phase

This section describes the message definitions for the HO Action Phase.

Table 4-94 – HO_Cnf (HO Confirm Type is Confirm or Unconfirmed)

IE	Reference	M/O	Notes	Applicability
HO Type	5.3.2.79	M		1.2.3
HO Confirm Type	5.3.2.76	M		1.2.3
MS Info	5.3.2.103	M		1.2.3
>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.	1.2.3
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1.2.3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1.2.3
>Authenticator ID	5.3.2.19	O	MAY be included if it is not sent during the HO Preparation phase.	1.2.3
>Anchor ASN GW ID	5.3.2.10	O	MAY be included if it is not sent during the HO Preparation phase.	1.2.3

IE	Reference	M/O	Notes	Applicability
>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.	1.2.3
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.	1.2.3
>SBC Context	5.3.2.174	O[1]	802.16e related MS session context.	1.2.3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2,
>>>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.	1,2,
>>>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.	1,2,
>>>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	1,2,
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>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.	1,2
>>PKM Flow Control	5.3.2.319	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Number of Supported Security Associations	5.3.2.320	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2,3
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>MAC Mode	5.3.2.322	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>Association type support	5.3.2.465	O		1,2
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Uplink Control Channel Support	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O		3
>>DEVICE_CLASS	5.3.2.504	O		3
>>CLC Request	5.3.2.505	O		3
>>Long TTI for DL	5.3.2.506	O		3
>>UL sounding	5.3.2.507	O		3
>>OL Region	5.3.2.508	O		3

IE	Reference	M/O	Notes	Applicability
>>DL resource metric for FFR	5.3.2.509	O		3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O		3
>>DL MIMO mode	5.3.2.512	O		3
>>feedback support for DL	5.3.2.513	O		3
>>Subband assignment A-MAP IE support	5.3.2.514	O		3
>>DL pilot pattern for MU MIMO	5.3.2.515	O		3
>>Number of Tx antenna of AMS	5.3.2.516	O		3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O		3
>>UL pilot pattern for MU MIMO	5.3.2.519	O		3
>>UL MIMO mode	5.3.2.520	O		3
>>Modulation scheme	5.3.2.521	O		3
>>UL HARQ buffering capability	5.3.2.522	O		3
>>DL HARQ buffering capability	5.3.2.523	O		3
>>AMS DL processing capability per sub-frame	5.3.2.524	O		3
>>AMS UL processing capability per sub-frame	5.3.2.525	O		3
>>FFT size(2048/1024/512)	5.3.2.526	O		3
>>Authorization policy support	5.3.2.21	O		3
>>Inter-RAT Operation Mode	5.3.2.527	O		3
>>Supported Inter-RAT type	5.3.2.528	O		3
>>MIH Capability Supported	5.3.2.529	O		3

IE	Reference	M/O	Notes	Applicability
>REG Context	5.3.2.144	O[1]	802.16e related MS session context.	1,2,3
>>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.	1,2
>>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.	1,2
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>DSx Flow Control	5.3.2.294	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>Maximum MAC Data per Frame Support	5.3.2.296	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>>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.	1,2
>>>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.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC ertPS Support	5.3.2.300	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O		3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O		3
>>Multicarrier capabilities	5.3.2.485	O		3
>>Zone Switch Mode Support	5.3.2.486	O		3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O		3
>>Interference mitigation supported	5.3.2.488	O		3
>>E-MBS capabilities	5.3.2.489	O		3
>>Channel BW and Cyclic prefix	5.3.2.490	O		3
>>frame configuration to support legacy R1.0	5.3.2.491	O		3
>>Persistent Allocation support	5.3.2.492	O		3
>>Group Resource Allocation support	5.3.2.493	O		3
>>Co-located coexistence capability support	5.3.2.494	O		3
>>HO Trigger Metric Support	5.3.2.326	O		3
>>EBB Handover support	5.3.2.495	O		3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O		3
>>Capability for sounding antenna switching support	5.3.2.497	O		3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O		3
>>ROHC support	5.3.2.499	O		3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O		3
>SA Descriptor	5.3.2.170	O[1]	SHOULD be included by Serving ASN for the Target ASN.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>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/ABS supports Mobility Restriction for stationary access and the MS mobility access classifier is known at the BS/ABS.	1,2,3
>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.	1,2,3
>SF Info (one or more)	5.3.2.185	M	It is included if TEK or Data Integrity information needs to be delivered.	1,2,3
>>SFID	5.3.2.184	M		1.2.3
>>SF Type	5.3.2.306	O		1.2.3
>>Direction	5.3.2.59	M	Specifies the direction of the flow.	1.2.3
>> CS Type	5.3.2.39	O	This TLV must be included in the transmitted message for the target ASN to setup flow	1.2.3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1.2
>>>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.	1.2
>>>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.	1.2
>>>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	1.2
>>ARQ Enable	5.3.2.345	O	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.	1.2,3
>>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.	1.2
>>>ARQ WINDOW SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1.2

IE	Reference	M/O	Notes	Applicability
>>>ARQ RETRY TIMEOUT-Transmitter Delay	5.3.2.347	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ RETRY TIMEOUT-Receiver Delay	5.3.2.348	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ BLOCK LIFETIME	5.3.2.349	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ SYNC LOSS TIMEOUT	5.3.2.350	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ DELIVER IN ORDER	5.3.2.351	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ RX PURGE TIMEOUT	5.3.2.352	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ BLOCK SIZE	5.3.2.353	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>RECEIVER ARQ ACK PROCESSING TIME.	5.3.2.354	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>SN Feedback Enabled field	5.3.2.468	O		1.2
>>FSN Size	5.3.2.469	O		1.2
>>CID	5.3.2.29	O		1.2
>>SAID	5.3.2.169	O		1.2.3
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O	The TLV SHALL be included for active service flows. This parameter is optional for the service flows that are not already activated.	1.2.3
>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule. This TLV SHALL be included if the *Packet Classification Rule / Media Flow Description* TLV is included in the transmitted message.	1.2.3
>>>Classification Rule Priority	5.3.2.32	CM	This TLV SHALL be included if the *Packet Classification Rule / Media Flow Description* TLV is included in the transmitted message.	1.2.3

IE	Reference	M/O	Notes	Applicability
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.	1.2.3
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...	1.2.3
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.	1.2.3
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.	1.2.3
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.	1.2.3
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.	1.2.3
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.	1.2.3
>>>IPv6 Flow Label	5.3.2.470	O		1.2.3
>>QoS Parameters	5.3.2.141	M		1.2.3
>>> DSCP	5.3.2.409	O	TC bit is set to 1	1.2.3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1.2.3
>>>>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.	1.2.3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1.2.3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2.3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1.2.3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.	1.2.3
>>>>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.	1.2.3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1.2.3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1.2.3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1.2.3
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.	1.2.3

IE	Reference	M/O	Notes	Applicability
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2.3
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1.2.3
>>>>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.	1.2.3
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1.2.3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1.2.3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1.2.3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2.3
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.	1.2.3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.	1.2.3
>>>> 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.	1.2.3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data Delivery Service is included in the transmitted message.	1.2.3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1.2.3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1.2.3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1.2.3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2.3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1.2.3
>>>>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.	1.2.3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1.2.3

IE	Reference	M/O	Notes	Applicability
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1.2.3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1.2.3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1.2.3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1.2.3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1.2.3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2.3
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1.2.3
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1.2.3
>>>Media Flow Type	5.3.2.94	O		1.2.3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1.2.3
>>>Reduced Resources Code	5.3.2.237	O		1.2.3
Refresh IP address trigger	5.3.2.375	O	Included for the BS/ABS to trigger IP address refresh on the MS via HO Process Optimization/Reentry Process Optimization TLV Bit #13. Currently used only for Simple IP re-anchoring.	1.2.3
>>PHS Rule	5.3.2.127	O		1.2.3
>>>PHSI	5.3.2.125	O	This TLV shall be included if PHS Rule is included in the transmitted message.	1.2.3
>>>PHSS	5.3.2.129	O		1.2.3
>>>PHSF	0	O		1.2.3
>>>PHSM	5.3.2.126	O		1.2.3
>>>PHSV	5.3.2.130	O		1.2.3
BS Info (Serving)	5.3.2.26	M		1.2.3
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.	1.2.3
>BS ID	5.3.2.25	M		1.2.3

IE	Reference	M/O	Notes	Applicability
>PHY Carrier Index	5.3.2.543	O	Physical carrier index of the recommended T-ABS. This TLV Shall be included when T-ABS is not included in AAI-NBR-ADV message or is multicarrier ABS.	3
BS Info (Target)	5.3.2.26	M		1.2.3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2.3
>BS ID	5.3.2.25	M		1.2.3
>HO ID	5.3.2.205	O	MAY be included as optional reference if the Target ASN has previously sent it with *HO_Rsp*.	1.2
>STID	5.3.2.473	O	MAY be included as optional reference if the Target ASN has previously sent it with *HO_Rsp*.	3
>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/ABS does not support combining of AK Context and HO Control message, it ignores this TLV as well as its child TLV(s).	1.2,3
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2,3
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2,3
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2,3
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2,3
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2,3

Note [1] : This TLV SHALL be included either in HO_Req or in HO_Cnf message.

Table 4-95 – HO_Cnf (HO Confirm Type is Cancel or Reject)

IE	Reference	M/O	Notes	Applicability
HO Type	5.3.2.79	M		1.2,3

IE	Reference	M/O	Notes	Applicability
HO Confirm Type	5.3.2.76	M		1.2,3
BS Info (Serving)	5.3.2.26	M		1.2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.	1.2,3
>BS ID	5.3.2.25	M		1.2,3
BS Info (Target)	5.3.2.26	M		1.2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2,3
>BS ID	5.3.2.25	M		1.2,3
>HO ID	5.3.2.205	O	MAY be included as optional reference if the Target ASN has previously sent it with *HO_Rsp*.	1.2
>STID	5.3.2.473	O	MAY be included as optional reference if the Target ASN has previously sent it with *HO_Rsp*.	3

The content of the *Context_Req* from Target BS/ABS to Serving BS/ABS appears in Table 4-96.

Table 4-96 – Context_Req from Target BS/ABS to Serving BS/ABS

IE	Reference	M/O	Notes	Applicability
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.	3
Context Purpose Indicator	5.3.2.36	M	Set to MAC Context Retrieval. Optionally, may include AK Context Retrieval as well.	1.2,3
MS Info	5.3.2.103	CM		3
>STID	5.3.2.473	CM	Old STID assigned by the old Serving ABS. In case of uncontrolled handover between two ABSs, this TLV SHALL be included.	3
>Basic CID	5.3.2.479	CM	Basic CID assigned by the old Serving BS. In case of uncontrolled handover from the LZone of an ABS to the MZone, this TLV SHALL be included.	3
BS Info (Serving)	5.3.2.26	M		1.2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.	1.2,3
>BS ID	5.3.2.25	M		1.2,3
BS Info (Target)	5.3.2.26	M		1.2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2,3
>BS ID	5.3.2.25	M		1.2,3

The content of the *Context_Rpt* from the Serving BS/ABS to the Target BS/ABS appears in Table 4-97.

Table 4-97 – Context_Rpt from Serving BS/ABS to Target BS/ABS

IE	Reference	M/O	Notes	Applicability
R6_Context_ID	5.3.2.440	M	Unique MS R6 context identifier.	3
Failure Indication	5.3.2.69	O		1.2,3
Context Purpose Indicator	5.3.2.36	M	Set to MAC Context Retrieval. Optionally, may include AK Context Retrieval as well.	1.2,3
MS Info	5.3.2.103	M		1.2,3
>STID	5.3.2.473	CM	Old STID assigned by the old Serving ABS. In case of uncontrolled handover between two ABSs, this TLV SHALL be included.	3
>MSID	5.3.2.102	CM	AMS's real MAC address	3
>Basic CID	5.3.2.479	CM	Basic CID assigned by the old Serving BS. In case of uncontrolled handover from the LZone of an ABS to the MZone, this TLV SHALL be included.	3
>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.	1.2,3
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1.2,3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1.2,3
>Service Authorization Code	5.3.2.181	O		1.2,3
>Anchor ASN GW ID	5.3.2.10	O	Identifies the node that hosts the Anchor DP Function in the Anchor ASN. Included if the originator of *HO_Req* does not host the Anchor DP Function for the MS.	1.2,3

IE	Reference	M/O	Notes	Applicability
>Authenticator ID	5.3.2.19	O	Identifies the node that hosts Authenticator and Key Distributor Function. Included if the originator of the *HO_Req* does not host the Authenticator and Key Distributor Function for the MS.	1.2,3
>SBC Context	5.3.2.174	O	802.16e related MS session context.	1.2,3
>>HARQ Context (one or more)	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>Direction	5.3.2.59	O	Indicates the direction of the management connection.	1,2,
>>>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.	1,2,
>>>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.	1,2,
>>>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	1,2,
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>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.	1,2
>>PKM Flow Control	5.3.2.319	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Number of Supported Security Associations	5.3.2.320	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2,3

IE	Reference	M/O	Notes	Applicability
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>MAC Mode	5.3.2.322	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>Association type support	5.3.2.465	O		1,2
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2

IE	Reference	M/O	Notes	Applicability
>>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.	1,2
>>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.	1,2
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	O	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O		3
>>DEVICE_CLASS	5.3.2.504	O		3
>>CLC Request	5.3.2.505	O		3
>>Long TTI for DL	5.3.2.506	O		3
>>UL sounding	5.3.2.507	O		3
>>OL Region	5.3.2.508	O		3
>>DL resource metric for FFR	5.3.2.509	O		3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O		3

IE	Reference	M/O	Notes	Applicability
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O		3
>>DL MIMO mode	5.3.2.512	O		3
>>feedback support for DL	5.3.2.513	O		3
>>Subband assignment A-MAP IE support	5.3.2.514	O		3
>>DL pilot pattern for MU MIMO	5.3.2.515	O		3
>>Number of Tx antenna of AMS	5.3.2.516	O		3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O		3
>>UL pilot pattern for MU MIMO	5.3.2.519	O		3
>>UL MIMO mode	5.3.2.520	O		3
>>Modulation scheme	5.3.2.521	O		3
>>UL HARQ buffering capability	5.3.2.522	O		3
>>DL HARQ buffering capability	5.3.2.523	O		3
>>AMS DL processing capability per sub-frame	5.3.2.524	O		3
>>AMS UL processing capability per sub-frame	5.3.2.525	O		3
>>FFT size(2048/1024/512)	5.3.2.526	O		3
>>Authorization policy support	5.3.2.21	O		3
>>Inter-RAT Operation Mode	5.3.2.527	O		3
>>Supported Inter-RAT type	5.3.2.528	O		3
>>MIH Capability Supported	5.3.2.529	O		3
>REG Context	5.3.2.144	O	802.16e related MS session context.	1,2,3
>>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.	1,2

IE	Reference	M/O	Notes	Applicability
>>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.	1,2
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>DSx Flow Control	5.3.2.294	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>Maximum MAC Data per Frame Support	5.3.2.296	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>>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.	1,2
>>>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.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC ertPS Support	5.3.2.300	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	O	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O		3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O		3
>>Multicarrier capabilities	5.3.2.485	O		3

IE	Reference	M/O	Notes	Applicability
>>Zone Switch Mode Support	5.3.2.486	O		3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O		3
>>Interference mitigation supported	5.3.2.488	O		3
>>E-MBS capabilities	5.3.2.489	O		3
>>Channel BW and Cyclic prefix	5.3.2.490	O		3
>>frame configuration to support legacy R1.0	5.3.2.491	O		3
>>Persistent Allocation support	5.3.2.492	O		3
>>Group Resource Allocation support	5.3.2.493	O		3
>>Co-located coexistence capability support	5.3.2.494	O		3
>>HO Trigger Metric Support	5.3.2.326	O		3
>>EBB Handover support	5.3.2.495	O		3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O		3
>>Capability for sounding antenna switching support	5.3.2.497	O		3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O		3
>>ROHC support	5.3.2.499	O		3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O		3
>SA Descriptor (one or more)	5.3.2.170	O	SHOULD be included by Serving ASN for the Target ASN.	1,2,3
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>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/ABS supports Mobility Restriction for stationary access and the MS mobility access classifier is known at the BS/ABS.	1,2,3
>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.	1,2,3
>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.	1,2,3
>>SFID	5.3.2.184	M		1.2,3
>>SF Type	5.3.2.306	O		1.2,3
>>Direction	5.3.2.59	M	Specifies the direction of the flow.	1.2,3
>>CS Type	5.3.2.39	O	This TLV must be included in the transmitted message for the target ASN to setup flow.	1.2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1.2
>>>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.	1.2
>>>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.	1.2
>>>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	1.2
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.	1.2,3
>>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.	1.2
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1.2

IE	Reference	M/O	Notes	Applicability
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ_SYNC_LOSS_TIMEOUT	5.3.2.350	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>ARQ_BLOCK_SIZE	5.3.2.353	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1.2
>>SN Feedback Enabled field	5.3.2.468	O		1.2
>>FSN Size	5.3.2.469	O		1.2
>>CID	5.3.2.29	O		1.2
>>SAID	5.3.2.169	O		1.2,3
>>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.	1.2,3
>>>Classification Rule Index	5.3.2.30	O	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.	1.2,3
>>>Classification Rule Priority	5.3.2.32	O		1.2,3
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.	1.2,3
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...	1.2,3

IE	Reference	M/O	Notes	Applicability
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.	1.2,3
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.	1.2,3
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.	1.2,3
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.	1.2,3
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.	1.2,3
>>>IPv6 Flow Label	5.3.2.470	O		1.2,3
>>QoS Parameters	5.3.2.141	M		1.2,3
>>> DSCP	5.3.2.409	O	TC bit set to 1	1.2,3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1.2,3
>>>>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.	1.2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1.2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2,3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1.2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.	1.2,3
>>>>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.	1.2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1.2,3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1.2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1.2,3
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.	1.2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2,3

IE	Reference	M/O	Notes	Applicability
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1.2,3
>>>>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.	1.2,3
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1.2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1.2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1.2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2,3
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.	1.2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.	1.2,3
>>>> 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.	1.2,3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data Delivery Service is included in the transmitted message.	1.2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1.2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1.2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1.2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2,3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1.2,3
>>>>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.	1.2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1.2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1.2,3

IE	Reference	M/O	Notes	Applicability
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1.2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1.2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1.2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1.2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1.2,3
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1.2,3
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1.2,3
>>>Media Flow Type	5.3.2.94	O		1.2,3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1.2,3
>>>Reduced Resources Code	5.3.2.237	O		1.2,3
>>PHS Rule	5.3.2.127	O		1.2,3
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1.2,3
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1.2,3
>>>PHSF	0	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1.2,3
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1.2,3
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1.2,3
BS Info (Serving)	5.3.2.26	M		1.2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Serving.	1.2,3
>BS ID	5.3.2.25	M		1.2,3
BS Info (Target)	5.3.2.26	M		1.2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2,3
>BS ID	5.3.2.25	M		1.2,3

IE	Reference	M/O	Notes	Applicability
>AK Context	5.3.2.6	O		1.2
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1.2
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2

The content of *Path_Reg_Req* is shown in Table 4-98. If Pre-Registration took place prior to Registration, none of the optional TLVs specified below needs to be included in the message.

Table 4-98 – Path_Reg_Req

IE	Reference	M/O	Notes	Applicability
Registration Type	5.3.2.145	M		1.2,3
MS Info	5.3.2.103	M		1.2,3
>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.	1.2,3
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1.2,3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1.2,3
>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.	1.2,3

IE	Reference	M/O	Notes	Applicability
>SF Info (one or more)	5.3.2.185	M	R4 Tunneling granularity is per SF.	1.2,3
>>SFID	5.3.2.184	M		1.2,3
>>CID	5.3.2.29	O	It SHALL be included if the Anchor ASN allocates CID.	1.2
>>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.	1.2,3
>>>Data Path ID	5.3.2.44	O		1.2,3
>>>Tunnel Endpoint	5.3.2.194	O		1.2,3
BS Info (Target)	5.3.2.26	M	SHALL be included to provide reference to the Target BS/ABS.	1.2,3
>BS ID	5.3.2.25	M		1.2,3

The content of Path_Reg_Rsp is shown in Table 4-98. If Pre-Registration took place prior to Registration, none of the optional TLVs specified below needs to be included in the message.

Table 4-99 – Path_Reg_Rsp

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1.2,3
Registration Type	5.3.2.145	M		1.2,3
MS Info	5.3.2.103	M		1.2,3
>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.	1.2,3
>SF Info (one or more)	5.3.2.185	M	R4 Tunneling granularity is per SF.	1.2,3
>>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.	1.2,3
>>>Data Path ID	5.3.2.44	O		1.2,3
>>>Tunnel Endpoint	5.3.2.194	O		1.2,3
>>SDU Info	5.3.2.176	O		1.2,3
>>>SDU SN	5.3.2.178	CM		1.2,3
BS Info (Target)	5.3.2.26	M		1.2,3
>BS ID	5.3.2.25	M		1.2,3

The content of *Path_Reg_Ack* is shown in Table 4-100.

Table 4-100 – Path_Reg_Ack

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1.2,3

The content of the *CMAC_Key_Count_Update* appears in Table 4-101.

Table 4-101 – CMAC_Key_Count_Update

IE	Reference	M/O	Notes	Applicability
MS Info	5.3.2.103	M	Contains HO-related MS context in the nested IEs.	1.2,3
> CMAC_KEY_COUNT	5.3.2.34	M	Delivers the CMACv2 Counter to the Authenticator.	1.2,3
>Authenticator ID	5.3.2.19	M		1.2,3
BS Info	5.3.2.26	M		1.2,3
>BS ID	5.3.2.25	M		1.2,3
Idle Mode Exit Indicator	5.3.2.369	O	This SHALL be included during Idle Mode Exit procedure.	1.2,3

The content of CMAC_Key_Count_Update_Ack is shown in Table 4-102.

Table 4-102 – CMAC_Key_Count_Update_Ack

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1.2,3
MS Info	5.3.2.103	M		1.2,3
>Authenticator ID	5.3.2.19	M	Authenticator ID for the MS.	1.2,3
BS Info	5.3.2.26	M		1.2,3
>BS ID	5.3.2.25	M		1.2,3

The content of the HO Complete from selected Target ASN to Serving ASN appears in Table 4-103.

Table 4-103 – HO Complete

IE	Reference	M/O	Notes	Applicability
Result Code	5.3.2.154	M	Result of the HO.	1.2,3

IE	Reference	M/O	Notes	Applicability
BS Info (Target)	5.3.2.26	M		1.2,3
> Serving/Target Indicator	5.3.2.182	M	Set to Target.	1.2,3
> BS ID	5.3.2.25	M	BS ID of the target where MS attempted to reenter in network.	1.2,3
MS Info	5.3.2.103	O	Contains HO-related MS context in the nested IEs. Mandatory only if sub-TLVs are present.	1.2,3
>SF Info	5.3.2.185	O		1.2,3
>>SFID	5.3.2.184	O	This TLV SHALL be included if SF Info is included in the transmitted message.	1.2,3
>>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.	1.2,3
>>>SDU SN	5.3.2.178	O	Last transmitted SDU sequence number. This TLV SHALL be included if SDU Info is included in the transmitted message	1.2,3

4.7.7 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/AMS located with the serving BS/ABS at the same ASN which convey both data and signaling information. The BS/ABSs SHALL be connected to the ASN GWs with R6 interfaces. The neighboring BS/ABSs 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/ABS and the Target BS/ABSs that reside in the same ASN and corresponding datapath establishment procedures over R6. R4 operations, if executed, are identical to those described in section 0. 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/ABS that hosts Serving HO Function and serves the MS/AMS prior to HO.

b. Target BS/ABS that hosts Target HO Function. There might be one or more Target BS/ABSs. One of them is selected as the final HO Target and becomes Serving BS/ABS 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/ABS. Target BS/ABS GW MAY be located on the path between the Anchor ASN GW and Target BS/ABS. 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 BS/ABSs and the Anchor GW goes directly over R6. In other words the BS/ABS and the Anchor GW reside at the same ASN

d. Authenticator ASN GW that hosts Authenticator/Key Distributor Function for the MS/AMS."

e. If R8 is not supported, or the Target BS/ABS 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/ABS 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.

In the case of R8 interface between BS and ABS, the applicable TLVs are indicated by applicability column in the message tables. Zone Switch is not supported for R8 handover cases.

4.7.7.1 Fully Controlled HO

4.7.7.1.1 HO Preparation Phase

Upon receipt of a MOB-MSHO_REQ/AAI-HO-REQ message from a mobile station (MS) or a advanced mobile station (AMS), or upon a decision to instigate Network Initiated HO, the Serving BS/ABS SHALL initiate a handover to one or more candidate Target BS/ABSs by sending a *HO_Req*(s) message to the Target BS/ABS(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/ABS(s) MAY retrieve AK Context and Service Authorization Info TLV from the Authenticator ASN GW. The Target BS/ABS(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 4-108.

Alternatively, the Serving BS/ABS MAY request on behalf of the Target BS/ABS the AK Context from the Authenticator ASN and include it in the *HO_Req* message

After receiving the *HO_Req* message, each Target BS/ABS MAY pre-establish the data path for the MS/AMS 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/ABS 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/ABS).

The Target BS/ABS SHALL respond to the *HO_Req* message with the *HO_Rsp* message, and the Serving BS/ABS SHALL acknowledge the Handover Preparation transaction completion by sending an *HO_Ack* message back to the Target BS/ABS(s).

4.7.7.1.1.1 R6 Data Path Pre-Registration Procedure

The procedure is identical to the one described in 4.12.1.2.

4.7.7.1.1.2 R6 Authenticator Context Retrieval Procedure

The procedure is identical to the one described in 4.12.2.2.

4.7.7.1.1.3 MS Initiated HO Preparation

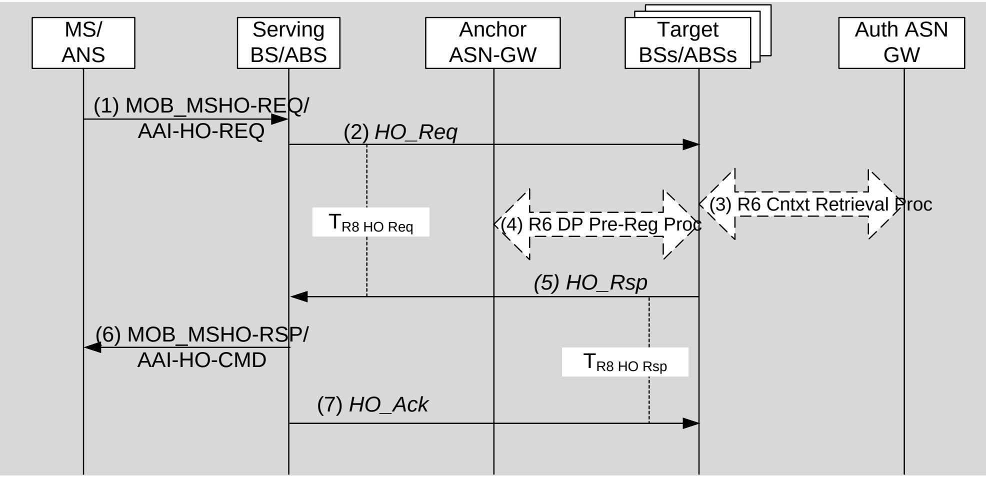


Figure 4-108 – Successful MS Initiated HO Preparation

STEP 1

The MS/AMS initiates a handover by sending a MOB_MSHO-REQ/AAI-HO-REQ message to the Serving BS/ABS, which may include one or more potential target BS/ABS's.

STEP 2

The Serving BS/ABS sends a *HO_Req* message destined to each potential Target BS/ABS's selected for the handover and starts timer $T_{R8\text{-}HO\ Req}$ or $T_{R6\text{-}HO\ Req}$ 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/AMS.

A Serving BS/ABS SHALL silently discard a duplicate MOB_MSHO-REQ/AAI-HO-REQ from an MS/AMS, if it has already initiated a HO preparation phase for this MS/AMS which is still ongoing. If a Serving BS/ABS receives such duplicate MOB_MSHO-REQ/AAI-HO-REQ from an MS/AMS, it SHALL not propagate the request further in to the network.

STEP 3

Upon receipt of the *HO_Req* message, the Target BS/ABS(s) MAY request AK context and service authorization information for the MS/AMS by initiating a Context Retrieval procedure with the Authenticator ASN GW. Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the Handover Action phase.

STEP 4

The Target BS/ABS(s) MAY initiate pre-establishment of a data path for the MS/AMS 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/ABS will be responded by the R6 *Path_Prereg_Rsp* message with an appropriate reject cause code. Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the handover Action Phase.

STEP 5

The Target BS/ABS(s) sends a *HO_Rsp* message to the Serving BS/ABS to acknowledge the handover request and starts timer $T_{R8\text{-}HO\ Rsp}$ or $T_{R6\text{-}HO\ Rsp}$ respectively. Upon receipt of the *HO_Rsp* message, the Serving BS/ABS stops timer $T_{R8\text{-}HO\ Req}$ or $T_{R6\text{-}HO\ Req}$ respectively.

STEP 6

The Serving BS/ABS sends a MOB_BSHO-RSP/AAI-HO-CMD message to the MS/AMS containing one or more potential target BS/ABS's selected by the Serving BS/ABS for the MS/AMS to handover to.

STEP 7

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS(s) controlling the potential target BS/ABS(s) selected for the MS/AMS. Upon receipt of the *HO_Ack* message, the Target BS/ABS(s) stops timer $T_{R8\text{-HO Rsp}}$ or $T_{R6\text{-HO Rsp}}$ respectively.

4.7.7.1.1.4 Network Initiated HO Preparation

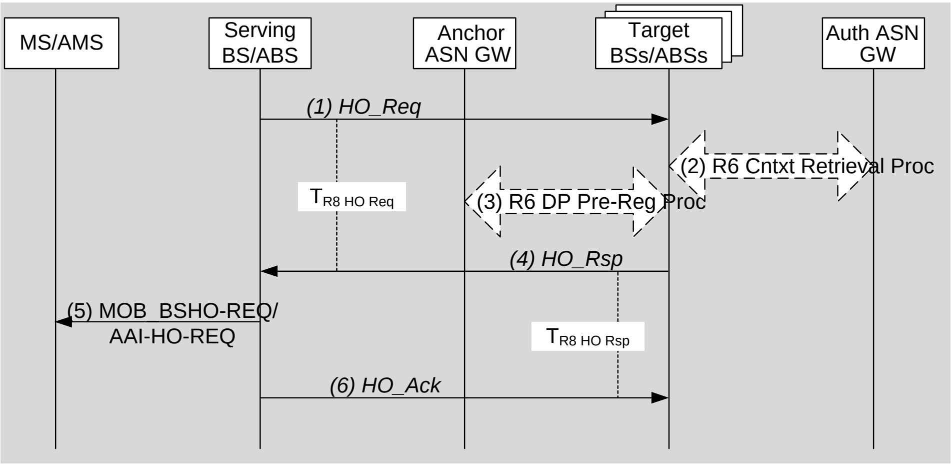


Figure 4-109 – Successful Network Initiated HO Preparation Phase

STEP 1

The Serving BS/ABS initiates a handover by sending a *HO_Req* message destined to each Target BS/ABS's selected for the handover and starts timer $T_{R8\text{-HO Req}}$ or $T_{R6\text{-HO Req}}$ 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/ABS(s) requests AK context and service authorization information for the MS/AMS by initiating a Context Retrieval procedure with the Authenticator ASN GW. Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the Handover Action phase.

STEP 3

The Target BS/ABS(s) MAY initiate pre-establishment of a data path for the MS/AMS 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/ABS will be responded by the R6 *Path_Prereg_Rsp* message with an appropriate reject cause code. Note: The Target BS/ABS(s) may optionally choose to defer this procedure to the handover action phase.

STEP 4

The Target BS/ABS(s) sends a *HO_Rsp* message to the Serving BS/ABS to acknowledge the handover request and starts timer $T_{R8\text{-HO Rsp}}$ or $T_{R6\text{-HO Rsp}}$ respectively. Upon receipt of the *HO_Rsp* message, the Serving BS/ABS stops timer $T_{R8\text{-HO Req}}$ or $T_{R6\text{-HO Req}}$ respectively.

STEP 5

The Serving BS/ABS sends a MOB_BSHO-REQ/AAI-HO-CMD message to the MS/AMS containing one or more potential target BS/ABS's selected by the network for the MS/AMS to handover to.

STEP 6

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS(s) controlling the potential target BS/ABS(s) selected for the MS/AMS. Upon receipt of the *HO_Ack* message, the Target BS/ABS(s) stops timer $T_{R8\text{-}HO\ Rsp}$ or $T_{R6\text{-}HO\ Rsp}$ respectively.

4.7.7.1.1.5 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:

– $T_{R8\text{-}HO\ Req}$: is started by a Serving BS/ABS upon sending the *HO_Req* message for an MS/AMS to a Target BS/ABS and is stopped upon receiving a corresponding *HO_Rsp* message from the Target BS/ABS.

– $T_{R8\text{-}HO\ Rsp}$: is started by a Target BS/ABS upon sending the *HO-Rsp* message for an MS/AMS to a Serving BS/ABS and is stopped upon receiving a corresponding *HO_Ack* message from the Serving BS/ABS.

R6 Timers are identical to those defined in 0.

Table 4-104 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-104 – HO Preparation Phase Timer Values for HO messages over R8

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R8\text{-}HO\ Req}$	TBD		TBD
$T_{R8\text{-}HO\ Rsp}$	TBD		TBD

4.7.7.1.1.6 HO Preparation Stage Error Conditions

This section describes error conditions associated with the HO Preparation Phase.

4.7.7.1.1.6.1 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 4-105.

Table 4-105 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{R8\text{-}HO\ Req}$	Serving BS/ABS	The Serving ASN may re-try HO to another Target BS/ABS. If no Target BS/ABS can be reached, the Serving BS/ABS SHALL send MS/AMS a MOB_BSHO-RSP/AAI-HO-CMD with Mode set to 0b111
$T_{R8\text{-}HO\ Rsp}$	Target BS/ABS	No Action required

4.7.7.1.1.6.2 HO_Rsp Error

Upon receipt of the *HO_Req* message, if the Target BS/ABS 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/ABS, the Serving BS/ABS SHALL stop $T_{R8\text{-}HO\_Req}$ or $T_{R6\text{-}HO\ Req}$ respectively (if running), and MAY re-send the *HO_Req* message to a different Target BS/ABS. If the Serving BS/ABS does not re-send the *HO_Req* message, or if all subsequent Target BS/ABSs cannot support the HO, in the case of MS Initiated handover, the Serving BS/ABS SHALL send either a MOB_BSHO_RSP with mode = 0b111: MS HO request not recommended (BS/ABS in list unavailable) or a AAI-HO-RSP with mode=0b10: AMS HO request rejected (ABS in list unavailable).

4.7.7.1.2 HO Action Phase

The HO Action Phase begins when the MS/AMS leaves the Serving BS/ABS. The MS/AMS sends a MOB_HO-IND/AAI-HO-IND message to the Serving BS/ABS in which it specifies which Target BS/ABS has been selected for the handover. The MOB_HO-IND/AAI-HO-IND message is the last message the MS/AMS sends to the Serving BS/ABS. After sending MOB_HO-IND/AAI-HO-IND the MS/AMS may start ranging with the Target BS/ABS.

In case that an AMS performs a handover between two ABSs and the AAI-HO-CMD message sent to an AMS during the HO Preparation phase contains only one candidate Target ABS which is accepted for the handover also by the AMS, the AMS shall move to the Target ABS without sending an AAI-HO-IND to the serving ABS.

Upon receiving MOB_HO-IND/AAI-HO-IND or at the designated Disconnect Time, the Serving BS/ABS SHALL generate a *HO_Cnf* message and send it to the Target BS/ABS. The *HO_Cnf* message includes the "most recent MAC context" at the Serving BS/ABS.

Upon receiving *HO_Cnf* message with the HO Indication type whose value is not set to "Cancel", or "Reject", the Target BS/ABS 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/ABS was not pre-established at the Preparation Phase, it MAY be pre-established after receiving *HO_Cnf* message and before the MS/AMS starts Network Re-Entry at the Target BS/ABS.

The data paths between the Anchor ASN GW and the Target BS/ABS SHALL be established via Data Path Registration procedure after the MS/AMS either starts or completes Network Re-Entry at the Target BS/ABS[17]. 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/AMS ID. In this case, all the parameters that are related to the data paths SHALL be exchanged during the

[17] If DP registration is initiated before MS/AMS completes Network Reentry there is a probability that MS/AMS 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

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 BS/ABSs 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/ABS and itself.

If the Serving BS/ABS determines that the MOB_HO_IND message was not received from the MS/AMS (due to a communication loss with the mobile[18], or of the message was corrupted), for example upon expiration of internal timer[19], the Serving BS/ABS 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 BS/ABSs that were indicated in the previous MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD message that was sent by the Serving BS/ABS to the MS/AMS. The *HO_Cnf* message may also be sent to Target BS/ABSs which weren't notified of a potential impending handover from the MS/AMS during the handover preparation phase and whose target BS/ABSs weren't included in the MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD messages (e.g. candidate Target BS/ABSs which were included in the MOB_MSHO-REQ/AAI-HO-REQ message sent by the MS/AMS but weren't notified of the handover in the handover preparation phase). Upon sending the *HO_Cnf* message to the candidate Target BS/ABS(s), the Serving BS/ABS SHALL stop all the downlink and uplink scheduling for the data transmission and reception from the MS/AMS respectively.

Upon sending the *HO_Cnf* message, if the Resource_Retain flag was not set, the Serving BS/ABS SHALL discard all MS/AMS's connections resource information including the MAC state machine and all outstanding buffered PDUs, else the Serving BS/ABS SHALL retain the connections, MAC state machine and PDUs associated with the MS/AMS for service continuation until the expiration of Resource Retain Timer.

The Serving BS/ABS MAY release all MAC context and MAC PDUs associated with the MS/AMS upon reception of a *HO Complete* message from the Target BS/ABS indicating MS/AMS committed Network Attachment at the Target BS/ABS.

If the Target BS/ABS does not receive the *HO_Cnf* message before the MS/AMS starts Network Reentry, the Target BS/ABS MAY request the "most recent MAC Context" via Context Request/Report exchange with the Serving BS/ABS as it is shown in Scenario 3.

Immediately after the MS/AMS completes Network Re-entry, the Target BS/ABS (which at that moment becomes new Serving BS/ABS) 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/ABS. The message SHALL deliver to the Authenticator the value of the CMAC_KEY_COUNT which is received from the MS/AMS. 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 Network Re-entry procedure at the Target BS/ABS is completed, the Target BS/ABS MAY send a *HO_Complete* message to the Serving BS/ABS to expedite the resource release in the Serving BS/ABS.

[18] MOB_HO-IND/AAI-HO-IND message could be lost over the air or not sent by the MS/AMS because it didn't receive the MOB_BSHO-RSP/AAI-HO-CMD message from the BS/TBS in the MS initiated handover case, or it didn't receive the MOB_BSHO-REQ/AAI-HO-CMD from the BS in the network initiated handover case.

[19] For example, $T_{MOB\_HO\_IND}$

4.7.7.1.2.1 R6 Data Path Registration Procedure

For HO over R8, the procedure is identical to the one described in 4.12.3.1.

4.7.7.1.2.2 R6 Data Path De-Registration Procedure

For HO over R8, the procedure is identical to the one described in 4.12.4.1

4.7.7.1.2.3 CMAC Key Count Update Procedure

For HO over R8, the procedure is identical to the one described in 4.12.5.2.

4.7.7.1.2.4 MAC Context Retrieval Procedure over R8

MAC Context Retrieval Procedure is shown in Figure 2:

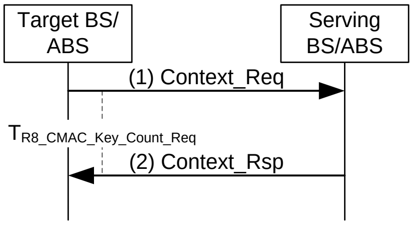


Figure 4-110 – MAC Context Retrieval Procedure

STEP 1

Target BS/ABS sends a *Context_Req* message to request the context associated with a specified MS/AMS stored in the Serving BS/ABS. The Target BS/ABS starts timer $T_{R8\text{-}Cntxt\_Req}$.

STEP 2

Serving BS/ABS responds by sending the requested context information for the mobile in the *Context_Rpt* message. Upon receipt of the *Context_Rpt* message, Target BS/ABS stops timer $T_{R8\text{-}Cntxt\_Req}$.

4.7.7.1.2.5 Handover Action Scenario 1: Serving BS/ABS Sends HO_Cnf message After receiving MOB HO-IND

The following call flow describes a successful handover action scenario where the Serving BS/ABS receives MOB-HO-IND/AAI-HO-IND and sends the *HO_Cnf* message to the Target BS/ABS.

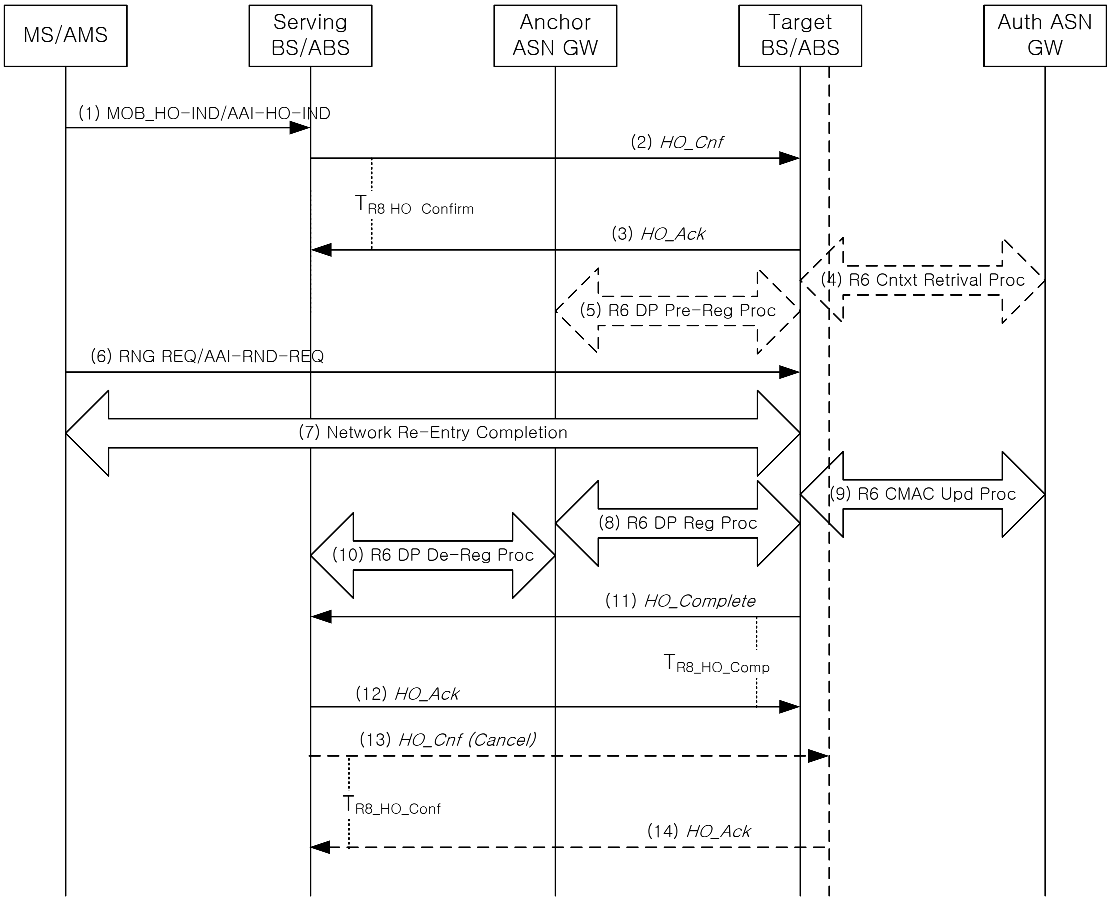


Figure 4-111 – Successful HO Action Phase, Scenario 1

STEP 1

The MS/AMS sends a MOB_HO-IND to the Serving BS/ABS to notify a handover to one of the Target BS/ABSs selected by the Serving BS/ABS in the Handover Preparation phase HO_IND_type field in the message is set to 0b00 (Serving BS/ABS Release).

STEP 2

Upon reception of the MOB_HO-IND/AAI-HO-IND the Serving BS/ABS sends a *HO_Cnf* message and starts timer $T_{R8\text{-HO Confirm}}$ or $T_{R6\text{-HO Confirm}}$ respectively. Serving BS/ABS MAY also send *HO_Cnf* message with the value of the HO_Indication type set to “Cancel” to all unselected Target BS/ABS(s) and clear the MS context.

STEP 3

The Target BS/ABS sends a *HO_Ack* message. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R8\text{-HO Confirm}}$ or $T_{R6\text{-HO Confirm}}$.

STEP 4

If AK context and service authorization information for the MS/AMS was not requested during the Handover Preparation phase, the Target BS/ABS requests AK context and service authorization information for the MS/AMS 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/AMS initiates network re-entry with the Target BS/ABS by sending an RNG-REQ/AAI-RNG-REQ in which the Serving BS/ABSID is included in the message and bit #0 is set to 1.

STEP 7

The Target BS/ABS responds with an RNG-RSP/AAI-RNG-RSP and the MS/AMS and the Target BS/ABS complete Network Reentry.

STEP 8

Target BS/ABS 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/ABS initiates CMAC Key Count Update procedure and updates the Authenticator ASN GW with the latest CMAC Key Count value received from MS/AMS.

STEP 10

Upon completing the Data Path Registration procedure with the Target BS/ABS, the Anchor ASN GW MAY initiates Data Path De-Registration procedure with the old Serving BS/ABS. Also, the Anchor ASN GW de-registers all the pre-registered data paths with the other unselected Target BS/ABSs. See discussion in 7.3.3.1.2.8 for more details.

STEP 11

Upon completion of network re-entry, the Target BS/ABS sends a *HO_Complete* message to notify the completion of the handover and starts timer $T_{R8\text{-HO Comp}}$ or $T_{R6\text{-HO Comp}}$ respectively. Upon receipt of the *HO_Complete* message, the Serving BS/ABS releases the MS context. If the Serving BS/ABS still has a data path with Anchor ASN GW, the Serving BS/ABS initiates Data Path De-Registration procedure (see section 7.3.3.1.2.8) with the Anchor ASN GW.

STEP 12

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS. Upon receipt of the *HO_Ack* message, the Target BS/ABS stops timer $T_{R8\_HO\_Comp}$ or $T_{R6\text{-HO Comp}}$ respectively.

STEP 13

Upon receiving *HO_Complete* message, if Serving BS/ABS did not send HO_Cnf message with the value of the HO_Indication type set to "Cancel" to all the unselected Target BS/ABS(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/ABS(s) to clear the MS context and starts timer $T_{R8\text{-HO Confirm}}$ or $T_{R6\text{-HO Confirm}}$ respectively.

STEP 14

Upon receipt of the *HO_Cnf(Cancel)* message the unselected Target BS/ABS(S) clear the MS context. The Target BS/ABS sends the *HO_Ack* message. Upon receipt of the *HO_Ack* the Serving BS/ABS stops timer $T_{R8\text{-HO Confirm}}$ or $T_{R6\text{-HO Confirm}}$ respectively.

4.7.7.1.2.6 Handover Action Scenario 2: Serving BS/ABS Proactively Sends HO_Cnf

The following call flow describes a successful handover action scenario where the Serving BS/ABS doesn't receive MOB_HO-IND/AAI-HO-IND and sends the *HO_Cnf* messages to the entire set of the Target BS/ABSs. See also section 4.7.7.1.2.7 HO Action Scenario 3.

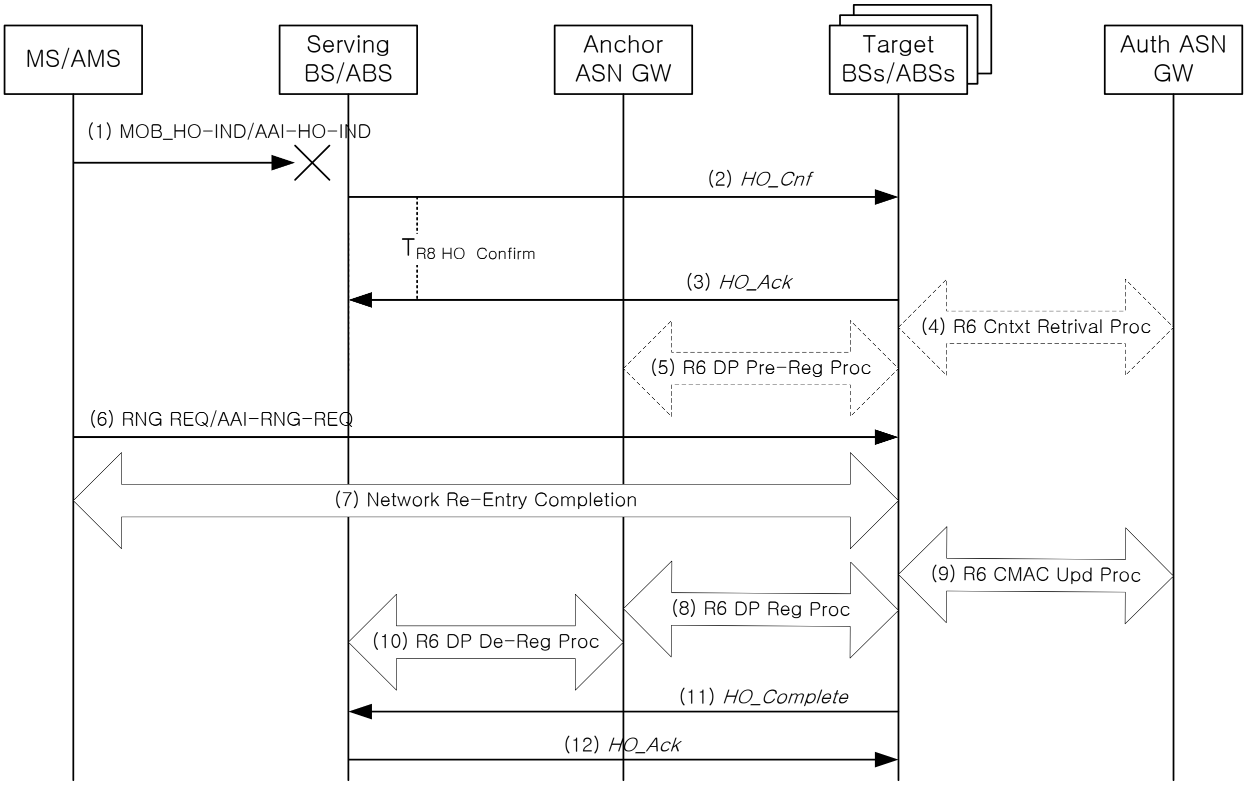


Figure 4-112 – Successful HO Action Phase, Scenario 2

The step description is the same as in Scenario 1 described in 4.7.7.1.2.5 with one difference – in this case in step 2, the serving BS/ABS sends multiple *HO_Cnf* messages. The *HO_Cnf* message may also be sent to candidate targets BS/ABSs the MS/AMS may choose to handover to which weren't previously notified of a potential handover from the MS/AMS 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/AMS.

4.7.7.1.2.7 Handover Action Scenario 3: Serving BS/ABS Doesn't Send R8 HO_Cnf

The following call flow describes a successful Handover Action scenario where the MOB_HO-IND/AAI-HO-IND sent by the MS/AMS to the Serving BS/ABS was lost over the air and not received by the Serving BS/ABS, and/or the *HO_Cnf* message sent by the Serving BS/ABS to the Target BS/ABS was either delayed or not received. The MS/AMS completes network re-entry at one of the Target BS/ABSs selected by the Serving BS/ABS during the Handover Preparation phase.

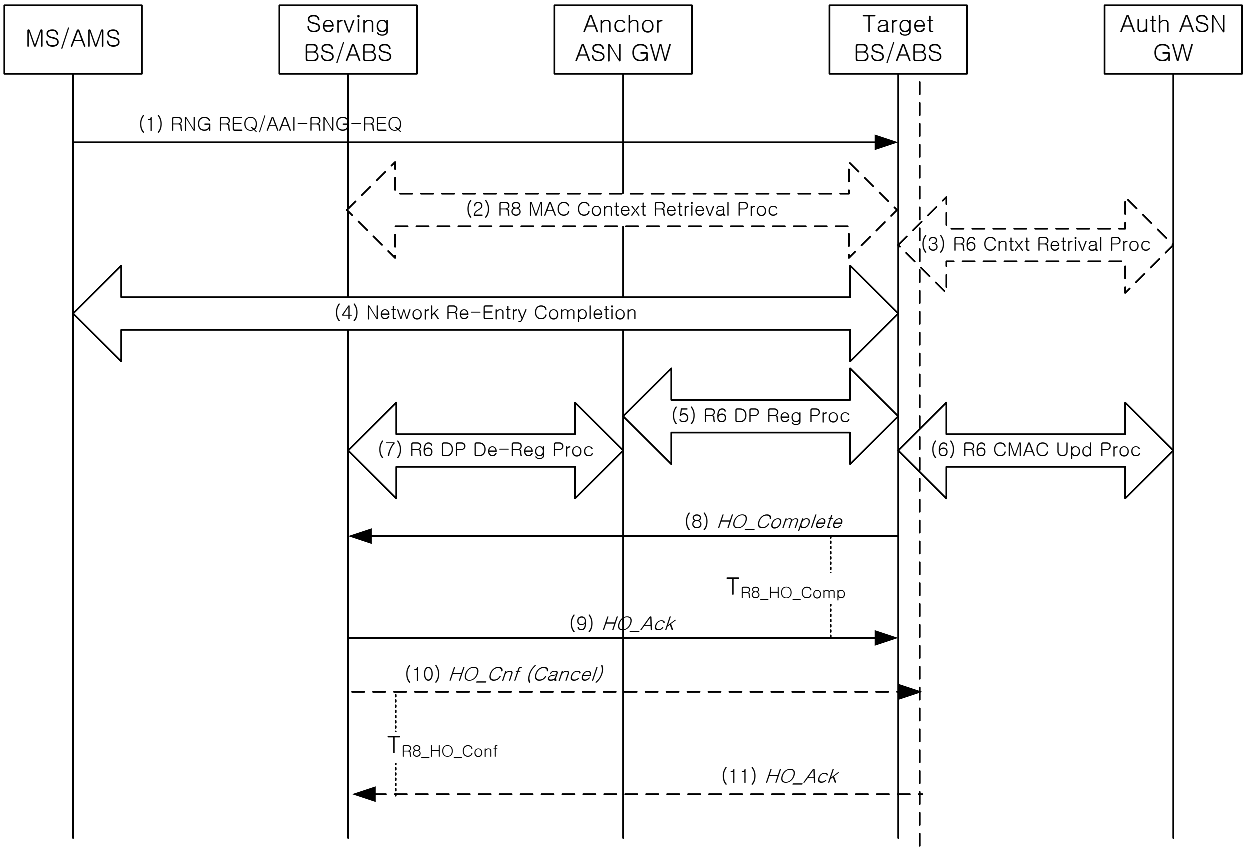


Figure 4-113 – Successful HO Action Phase, Scenario 3

STEP 1

The MS/AMS initiates network re-entry with the Target BS/ABS by sending RNG-REQ/AAI-RNG-REQ.

STEP 2

If the Target BS/ABS needs to synchronize the dynamic MAC context it initiates a Context Retrieval procedure with the Serving BS/ABS to retrieve the latest MAC context for the MS/AMS.

STEP 3

If AK context and service authorization information was not obtained during the Handover Preparation phase, the Target BS/ABS requests AK context and service authorization information for the MS/AMS by initiating a Context Retrieval 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/ABS responds with RNG-RSP/AAI-RNG-RSP and the MS/AMS and the Target BS/ABS complete Network Reentry.

STEP 5

Target BS/ABS 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/ABS initiates CMAC Key Count Update procedure and updates the Authenticator ASN GW with the latest CMAC Key Count value received from MS/AMS.

STEP 7

Upon completing the Data Path Registration procedure with the Target BS/ABS, the Anchor ASN GW MAY initiates Data Path De-Registration procedure with the old Serving BS/ABS. Also, the Anchor ASN GW SHALL de-register all the pre-registered data paths with the unselected Target BS/ABSs. See discussion in 7.3.3.1.2.8 for more details.

STEP 8

Upon completion of network re-entry, the Target BS/ABS sends a *HO_Complete* message to notify the completion of the handover. Upon receipt of the *HO_Complete* message, the Serving BS/ABS releases the MS context and starts timer $T_{R8\_HO\_Comp}$. or $T_{R6\text{-}HO\ Comp}$ respectively. If the Serving BS/ABS still has a data path with Anchor ASN GW, the Serving BS/ABS initiates Data Path De-Registration procedure (see section 7.3.3.1.2.8) with the Anchor ASN GW.

STEP 9

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R8\text{-}HO\ Comp}$. or $T_{R6\text{-}HO\ Comp}$ respectively.

STEP 10

The Serving BS/ABS may have already sent the *HO_Cnf* message with the HO_Indication type set to “Cancel” to some or all target BS/ABSs. For all unselected target BS/ABSs to which such message has not been sent yet, the Serving BS/ABS sends such a message upon receipt of *HO_Complete* message in order to clear the MS context at Target BS/ABSs. When the Serving BS/ABS sends *HO_Cnf* message it starts timer $T_{R8\_HO\_Confirm.}$ or $T_{R6\text{-}HO\ Confirm}$ respectively.

STEP 11

Upon receipt of the *HO_Cnf*(Cancel) message the Target BS/ABS(S) clear the MS context. The Target BS/ABS sends the *HO_Ack* message. Upon receipt of the HO_Ack message the Serving BS/ABS stops timer $T_{R8\text{-}HO\ Confirm}$ or $T_{R6\text{-}HO\ Confirm}$ respectively.

4.7.7.1.2.8 Path De-Registration with Old Serving and Unselected Target BS/ABSs

R6 Path Registration Procedure between the finally selected Target BS/ABS and Anchor ASN GW triggers R6 Path Deregistration of the Data Path between the Anchor ASN GW and the old Serving BS/ABS as well as between the Anchor ASN GW and each of the Unselected Target BS/ABSs. In the latter case the procedure takes place if the corresponding Data Paths were previously pre-registered. The scenario is shown in Figure 4-114.

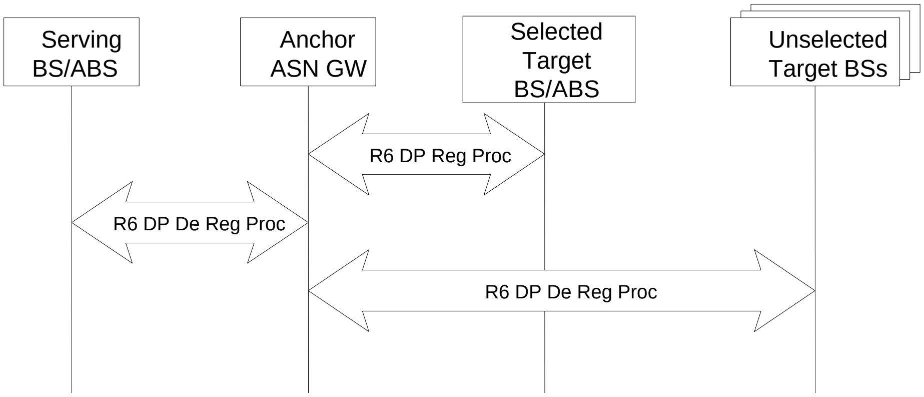


Figure 4-114 – Path De-Registration with Old Serving and Unselected Target BS/ABSs

All R6 Path Deregistration Procedures shown are independent of each other and may happen simultaneously.

4.7.7.1.2.9 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:

- $T_{R8\text{-HO Confirm}}$: is started by the Serving BS/ABS when sending a *HO_Cnf* message to a Target BS/ABS, and is stopped upon receiving a *HO_Ack* message from the corresponding Target BS/ABS.

R6 Timers are identical to those defined in 4.7.2.5.

Table 4-106 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-106 – HO Action Phase Timer Values for R8

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R8\text{-HO Confirm}}$	TBD		TBD
$T_{R8\_HO\_Comp}$	TBD		TBD

4.7.7.1.2.10 HO Action Phase Error Conditions

This section describes error conditions associated with the HO Action Phase.

4.7.7.1.2.10.1 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 4-107.

Table 4-107 – Timer Max retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{R8\text{-HO Confirm}}$	(old) Serving BS/ABS	TBD
$T_{R8\_HO\_Comp}$	Target BS/ABS (New Serving)	No action required

4.7.7.1.2.10.2 Context_Rpt Error

Upon receipt of the *Context_Req* message, if the Serving BS/ABS 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/ABS SHALL stop timer $T_{R8\text{-}Cntxt\_Req}$ or $T_{R6\text{-}Contxt}$ Req respectively (if running), and MAY resend the *Context_Req* message. If the Target BS/ABS 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.

4.7.7.1.3 HO Cancel

HO Cancellation is a variant of HO Action Phase, when the Serving BS/ABS signals to one or more Target BS/ABSs that the HO is to be cancelled. The HO Cancellation will be invoked only if the Target BS/ABS 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 BS/ABSs that have not been chosen as the final HO Target by the MS/AMS or to all the Target BS/ABSs when the MS/AMS has decided to cancel the HO procedure completely.

Note: The reference of “Unselected Target BS/ABS” below figures for various HO Cancellation scenarios is referred to the Target BS/ABS that was previously selected as the potential Target BS/ABS that MS/AMS may handover to, and some system resource may have been pre-allocated at the Target BS/ABS including the data path resources towards the Anchor ASN GW.

4.7.7.1.3.1 HO Cancellation Scenario 1: “Unselected BS” receives HO_Cnf from Serving BS/ABS

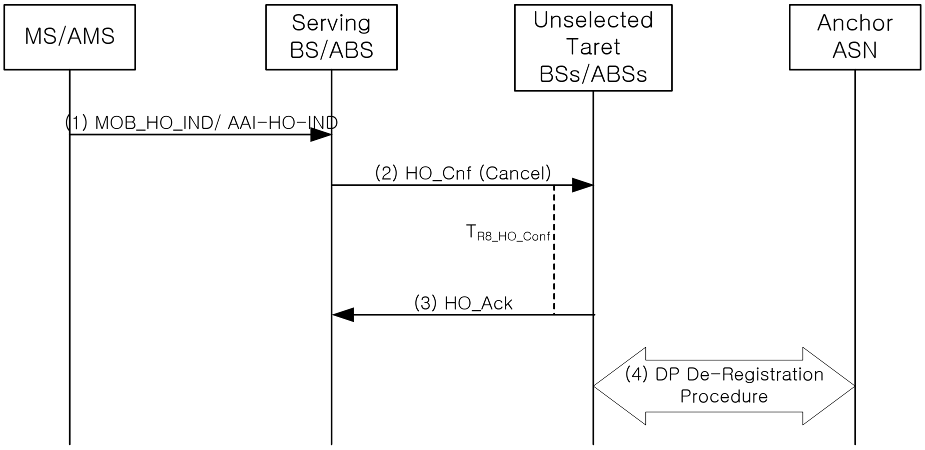

MS/AMS
Serving BS/ABS
Unselected Taret BSs/ABSs
Anchor ASN
(1) MOB_HO_IND/ AAI-HO-IND
(2) HO_Cnf (Cancel)
TR8_HO_Conf
(3) HO_Ack
(4) DP De-Registration Procedure

Figure 4-115 –HO Cancellation, Scenario 1

STEP 1

The MS/AMS sends MOB_HO-IND/AAI-HO-IND to the Serving BS/ABS. In the MOB_HO-IND/AAI-HO-IND, the MS/AMS indicates the Serving BS/ABS with two possibilities:

a) The selected Target BS/ABS that the MS/AMS chooses to perform the handover, or

b) The MS/AMS decides to cancel the handover procedures, in this case, the selected Target BS/ABS is the Serving BS/ABS

STEP 2

Receiving either the MOB_HO-IND with HO_IND_type set to 0b01: HO Cancel or the AAI-HO-IND with HO Event Code set to 0b11: HO Cancel causes the Serving BS/ABS to send *HO_Cnf* message with the value of HO_Indication type set to “Cancel” to inform the previously selected potential Target BS/ABS(s) which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD message to de-allocate the reserved system resources that are prepared for the MS/AMS to handover. After sending the message, the Serving BS/ABS awaits *HO_Ack* by starting the T_{HO_Conf}. If the timer expires, the Serving BS/ABS may re-send the *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS/ABS stops resending the *HO_Cnf*. The Target BS/ABS SHALL perform the local clean up if *HO_Cnf* is never received from the Serving BS/ABS.

STEP 3

Target BS/ABS receives the *HO_Cnf* with HO_Indication type set to “Cancel”. Target BS/ABS sends *HO_Ack* to the Serving BS/ABS and may release the pre-allocated system resources, which are to support the MS/AMS handover. .

STEP 4

The Target BS/ABS may send the R6 *Path_Dereg_Req* to the Anchor ASN GW if data path has already been established between the Target BS/ABS and the Anchor ASN GW. Target BS/ABS sets the timer $T_{R6\ Path\ Dereg\ Req}$ to wait for the response from the Anchor ASN GW. If the R6 *Path_DeReg_Rsp* is not received by the Target BS/ABS before the expiry of the $T_{R6\ Path\ Dereg\ Req}$, the Target BS/ABS may re-transmit the message until the maximum number of retransmissions. If the MS/AMS is no longer attached to the Serving BS/ABS, the Serving BS/ABS SHALL release all the allocated system resource for the MS/AMS.

4.7.7.1.3.2 HO Cancellation Scenario 2: "Unselected BS does not Receive HO_Cnf from Serving BS/ABS

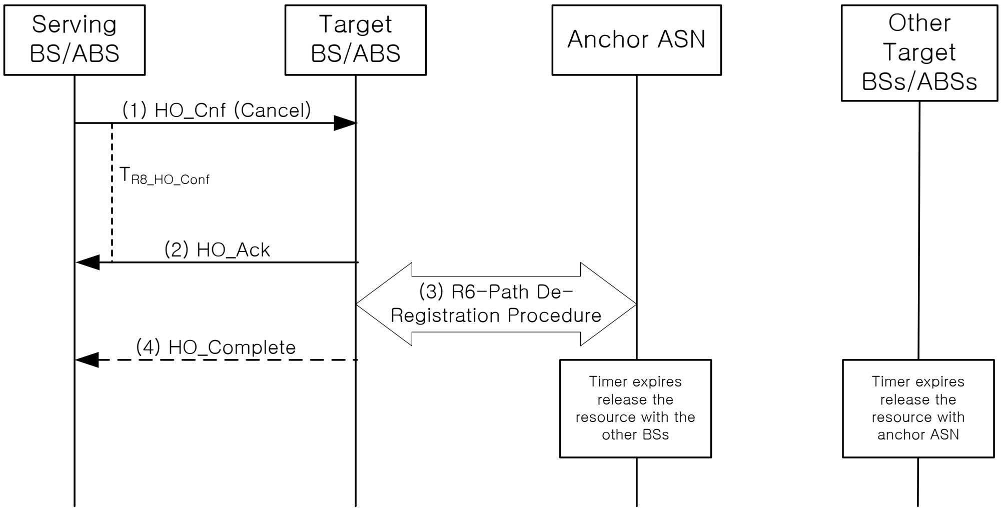

Serving BS/ABS
Target BS/ABS
Anchor ASN
Other Target BSs/ABSs
(1) HO_Cnf (Cancel)
$T_{R8\_HO\_Conf}$
(2) HO_Ack
(3) R6-Path De-Registration Procedure
(4) HO_Complete
Timer expires release the resource with the other BSs
Timer expires release the resource with anchor ASN

Figure 4-116 –HO Cancellation, Scenario 3

The MS/AMS sends an MOB_HO-IND/AAI-HO-IND to the Serving BS/ABS. In the MOB_HO-IND/AAI-HO-IND, the MS/AMS indicates the Serving BS/ABS with two possibilities:

- The selected Target BS/ABS that the MS/AMS chooses to perform the handover, or
- The MS/AMS decides to cancel the handover procedures, in this case, the selected Target BS/ABS is the Serving BS/ABS

STEP 1

Receiving either the MOB_HO-IND with HO_IND_type set to 0b01: HO Cancel or the AAI-HO-IND with HO Event Code set to 0b11: HO Cancel causes the Serving BS/ABS to send *HO_Cnf* message with the value of HO_Indication type set to "Cancel" to inform the previously selected potential Target BS/ABS(s) which are indicated in the MOB_BSHO-REQ or MOB_BSHO-RSP or AAI-HO-CMD message to de-allocate the reserved system resources that are prepared for the MS/AMS to handover. After sending the message, the Serving BS/ABS awaits *HO_Ack* by starting the $T_{R8\_HO\_Conf\_}$ or $T_{R6\_HO\_Conf}$ respectively. If the timer expires, the Serving BS/ABS may re-send the *HO_Cnf*. After a pre-defined number of retransmissions, the Serving BS/ABS stops resending the *HO_Cnf*. The Target BS/ABS SHALL perform the local clean up if *HO_Cnf* is never received from the Serving BS/ABS.

STEP 2

The Target BS/ABS does not receive the *HO_Cnf*. The Target BS/ABS releases the pre-allocated system resources which are to support the MS/AMS handover.

STEP 3

After the timer associated with the pre-registered DP expires, the Target BS/ABS may send the R6 *Path_Dereg_Req* to the Anchor ASN GW if a data path has already been established between the Target BS/ABS and the Anchor ASN GW. The Target BS/ABS sets the timer $T_{R6\ Path\ Dereg\ Req}$ to wait for the response from the Anchor ASN GW. If the R6 *Path_DeReg_Rsp* is not received by the Target BS/ABS before the expiry of the $T_{R6\ Path\ Dereg\ Req}$, the Target BS/ABS may re-transmit the message until the maximum number of retransmissions. . If the MS/AMS is no longer attached to the Serving BS/ABS, the Serving BS/ABS SHALL release all the allocated system resource for the MS/AMS.

4.7.7.1.4 HO Reject

The following call flow describes the scenario when the MS/AMS rejects Target BS/ABSs offered to it by the Serving BS/ABS for handover.

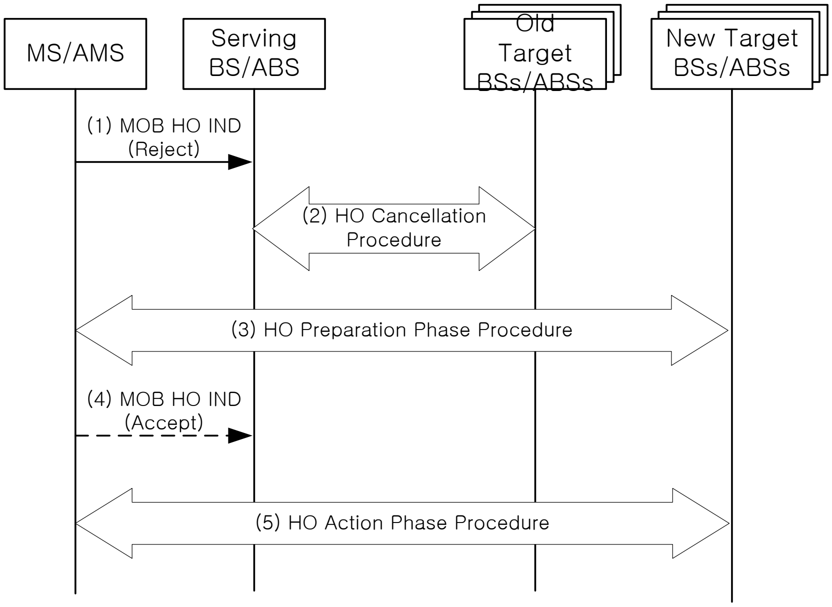


Figure 4-117 – HO Reject

1. The MS/AMS sends a MOB_HO-IND containing HO_IND_Type TLV set to 0b10 indicating rejection of the Target BS/ABS(s) offered by the Serving BS/ABS for handover in the MOB_BSHO-RSP (MS initiated handover) or MOB_BSHO-REQ (network initiated handover) message.
2. The Serving BS/ABS initiates the handover cancellation procedures described in section 4.7.2.3 with the Target BS/ABS(s) which were rejected for handover by the MS/AMS.

The following steps only occur if the Serving BS/ABS is able to offer an alternate Target BS/ABS(s) to the MS/AMS.

3. The Serving BS/ABS initiates the handover preparation procedure with a Target BS/ABS(s) or through Relay ASN-GW(s) controlling a new candidate Target BS/ABS(s) to be offered to the MS/AMS for handover.
4. The MS/AMS indicates acceptance of a new Target BS/ABS offered by the Serving BS/ABS to the MS/AMS for handover in the MOB_BSHO-RSP or MOB_BSHO-REQ message by sending a MOB_HO-IND message with HO_IND_Type TLV set to 0b00.
5. The Serving BS/ABS completes the handover action procedures described in section 4.7.2.2 and the MS/AMS completes successful handover to the new Target BS/ABS.

Note: If the MS/AMS rejects the Target BS/ABS offered by the Serving BS/ABS as described in step 1, steps 1-2 are repeated. If the Serving BS/ABS decides to offer a new Target BS/ABS for handover to the MS/AMS, steps 3-5 are repeated.

4.7.7.2 Uncontrolled HO

An Uncontrolled (Unpredictive) handover occurs when an MS/AMS starts ranging at a Target BS/ABS that wasn't previously notified of an impending handover from an MS/AMS and didn't participate in the Handover Preparation Phase. This may occur due to suboptimal radio planning conditions or MS/AMS implementation (handover notification of the Serving BS/ABS by MS/AMS is optional).

If an MS/AMS starts ranging with a BS/ABS that doesn't have MS Context information including Authenticator GW and Anchor ASN GW identifiers, the RNG-REQ/AAI-RNG-REQ message from the MS/AMS cannot be authenticated. In a worst case scenario a full Network Re-Entry will be required which results in a large delay, 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/AMS includes the Serving BS/ABS ID TLV in the RNG-REQ/AAI-RNG-REQ message, the handover can still be completed in a reasonable delay and the period of traffic unavailability can be greatly reduced. When an MS/AMS re-enters at a Target BS/ABS and supplies its Serving BS/ABS ID in the RNG-REQ/AAI-RNG-REQ message, the Target BS/ABS may retrieve the relevant MS Context from the Serving BS/ABS including the Authenticator GW ID and Anchor ASN GW ID. Thus it becomes possible for the Target BS/ABS to authenticate the RNG-REQ/AAI-RNG-REQ and perform data path registration with the Anchor ASN GW. This call flow scenario is described in Figure 4-118.

Network Re-Entry might be completed immediately after receiving the MS Context or after data path establishment (the former case is shown in the call flows). The former method requires a lower Ranging Response Timeout in the MS/AMS, 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/AMS. The moment of Network Re-Entry completion does not affect interoperability and is left as a vendor implementation option.

The following call flow provides an example of a successful uncontrolled handover scenario. An MS/AMS begins ranging at the Target BS/ABS that wasn't contacted by the Serving BS/ABS to participate in the Handover Preparation phase. Therefore the Target BS/ABS was unaware of an impending arrival of the MS/AMS. The Target BS/ABS retrieves the MS context and authenticator information and successfully completes the handover.

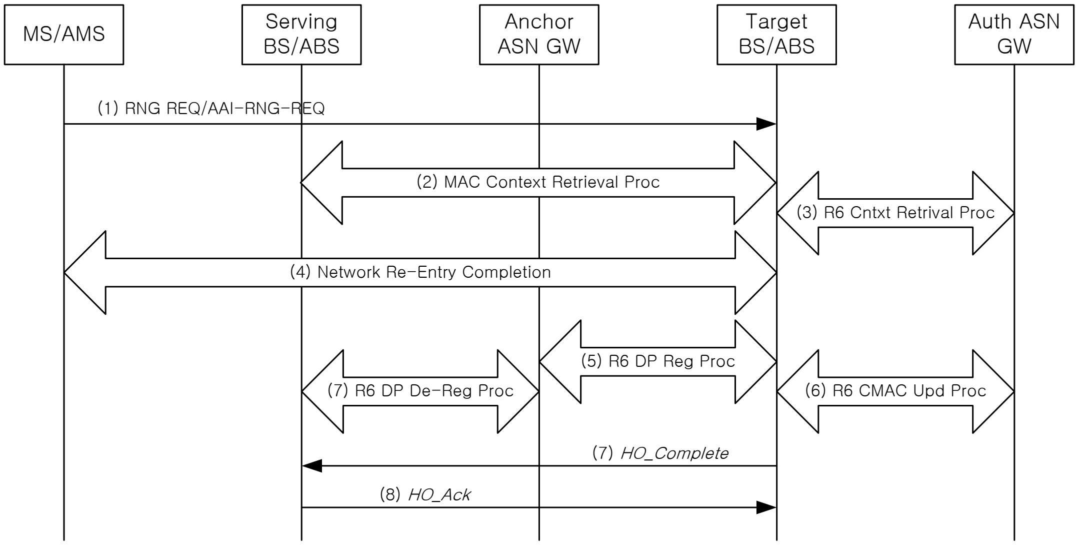


Figure 4-118 – Uncontrolled (Unpredictive) HO

STEP 1

An MS/AMS performs an uncontrolled handover by sending an RNG-REQ message to perform contention based ranging at a Target BS/ABS that didn't receive prior notification of an impending handover from the MS/AMS and therefore didn't participate in the Handover Preparation phase. The MS/AMS includes the Serving BS/ABSID TLV in the RNG-REQ/AAI-RNG-REQ message.

STEP 2

The Target BS/ABS initiates a MAC context retrieval procedure with the Serving BS/ABS to retrieve context information for the MS/AMS. The Serving BS/ABS responds by sending the context information that includes the Authenticator ASN GW ID and Anchor ASN GW ID.

STEP 3

The Target BS/ABS requests AK context and service authorization info for the MS/AMS by initiating a Context Retrieval procedure with the Authenticator ASN GW.

STEP 4

Target BS/ABS uses the Authenticator context to authenticate the MS/AMS message. The Target BS/ABS sends a RNG-RSP/AAI-RNG-RSP message to the MS/AMS acknowledging the HMAC/CMAC tuple (expedited security authentication) and containing the HO Process Optimization/Reentry Process Optimization TLV.

STEP 5

The Target BS/ABS initiates data path registration for the MS/AMS with the Anchor ASN GW. Note: This step may occur any time after step 3.

STEP 6

Upon successful completion of MS network re-entry, the Target BS/ABS 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/ABS.

STEP 8

Upon completion of network re-entry, the Target BS/ABS SHALL send a *HO_Complete* message to notify the completion of the handover. Upon receipt of the *HO_Complete* message, the Serving BS/ABS releases the MS context and starts timer $T_{R8\text{-HO Comp}}$ or $T_{R6\text{-HO Comp}}$ respectively.

STEP 9

The Serving BS/ABS sends a *HO_Ack* message to the Target BS/ABS. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R8\_HO\_Comp}$ or $T_{R6\text{-HO Comp}}$ respectively.

4.7.7.3 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/ABS ID SHALL be included in the messages sent over R6 or R8.

4.7.8 Data Integrity

4.7.8.1 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/ABS, Target BS/ABS 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.

4.7.8.2 Data Paths during handover

Before handover, Data Path(s) exists only between the Anchor ASN GW and the Serving BS/ABS (solid line in the Figure 4-119). 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 BS/ABSs are pre-established then the resulting Data Paths will take the form of a tree as it appears in Figure 4-119.

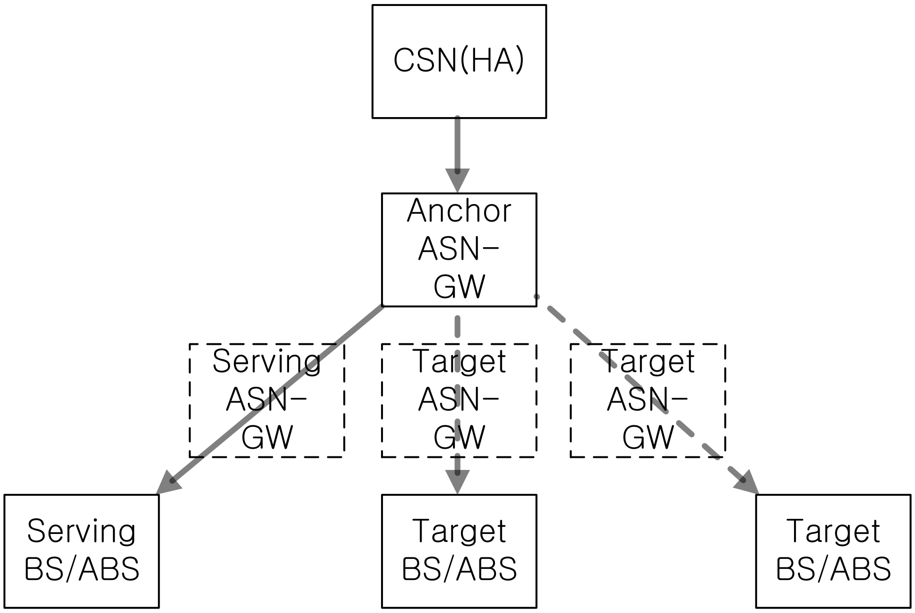


Figure 4-119 – Per SF Data Path Tree after HO Preparation Phase

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/ABS for later delivery on demand, to Target BS/ABS.

4.7.8.3 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/ABS and Target BS/ABS, the ARQ State Machine (for ARQ enabled Service Flows) at MS/AMS and Target BS/ABS SHALL be automatically reset after handover without any explicit ARQ reset notification. The MS/AMS 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/Reentry Process Optimization" bitmask that is delivered to the MS/AMS over the air. The Target BS/ABS transmits "HO Process Optimization/Reentry Process Optimization" bitmask in RNG-RSP/AAI-RNG-RSP. The Serving BS/ABS transmits 'HO Process Optimization/Reentry Process Optimization' bitmask in MOB_BSHO-RSP or MOB_BSHO-REQ or AAI-HO-CMD. 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.

4.7.8.3.1 Downlink Data Integrity Methods

This section describes each specific method that can be applied for downlink data integrity support during handover.

4.7.8.3.1.1 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 BS/ABSs. 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/ABS 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.

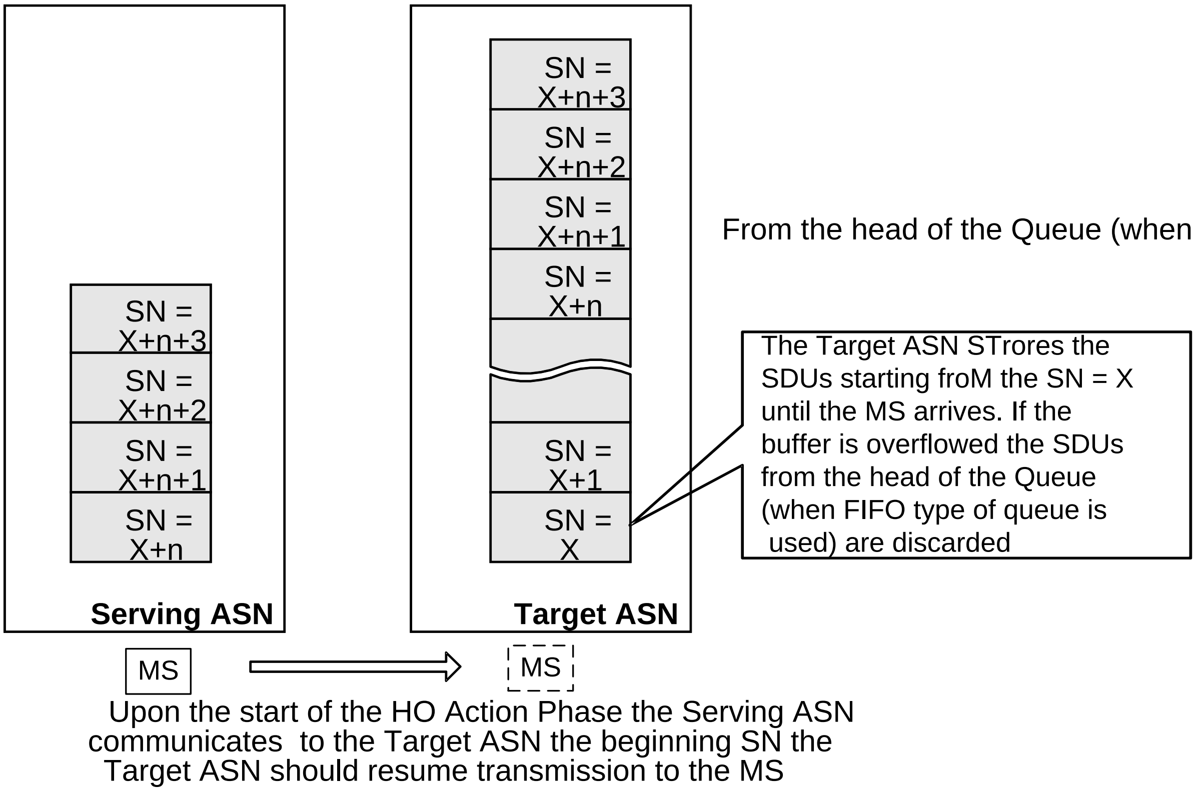

SN = X+n+3
SN = X+n+2
SN = X+n+1
SN = X+n
Serving ASN
SN = X+n+3
SN = X+n+2
SN = X+n+1
SN = X+n
SN = X+1
SN = X
Target ASN
From the head of the Queue (when
The Target ASN STrores the SDUs starting froM the SN = X until the MS arrives. If the buffer is overflowed the SDUs from the head of the Queue (when FIFO type of queue is used) are discarded
MS
MS
Upon the start of the HO Action Phase the Serving ASN communicates to the Target ASN the beginning SN the Target ASN should resume transmission to the MS

Figure 4-120 – Transmission Queues in Serving BS/ABS and Target BS/ABS

Case: Data Path Setup from Target BS/ABS: 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 BS/ABSs 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/ABS reports this SN to the Serving BS/ABS, so the latter knows which part of data is available in each Target BS/ABS. The Serving BS/ABS may then use this knowledge in order to deliver the data that are not yet available in the Target BS/ABSs to the MS/AMS prior to confirming handover with MOB_BSHO-RSP/AAI-HO-CMD or initiating handover with MOB_BSHO-REQ/AAI-HO-CMD.

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/ABS reports the SN to the Serving BS/ABS, so the latter knows which part of data is available in each Target BS/ABS. The Serving BS/ABS may then use this knowledge in order to deliver the data that are not yet available in the Target BS/ABSs.

Delivering the SN of the first multi-unicast SDU from the Target BS/ABS to the Serving BS/ABS is optional and may be omitted.

SDU Transfer: The Target BS/ABSs store the data until either the MS/AMS arrives or the handover is cancelled. The Figure 4-120 shows an example where multi-unicasting for a particular Service Flow started from the SDU with SN = X. Thus each Target BS/ABS 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/ABS, it may discard the SDUs from the head of the Queue.

Meanwhile the Serving BS/ABS keeps transmitting the data to the MS/AMS. In Figure 4-120 it has transmitted n SDUs and the SDU with SN = X+n is at the head of the Transmission Queue. If the MS/AMS sends MOB_HO-

IND/AAI-HO-IND at this moment or the Disconnect Time has been reached, the Serving BS/ABS will report to the Target BS/ABS (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 4-120. 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/AMS. If MOB_HO-IND /AAI-HO-IND has never been received in the Serving BS/ABS and thus *HO_Cnf* message has never been sent then the Target BS/ABS may retrieve the same information using Context Retrieval Transaction.

Thus the Target BS/ABS 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/AMS send SDU SN Feedback Header with the last SDU SN (SN = X+n) on the uplink channel to the Target ASN as described in 4.7.8.3.3.

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/ABS).

It may happen that the Transmission Queue in the Serving BS/ABS consists of partially delivered (partially acknowledged) SDUs interleaved with fully delivered SDUs. For example the Serving BS/ABS 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 4-121 illustrates the example.

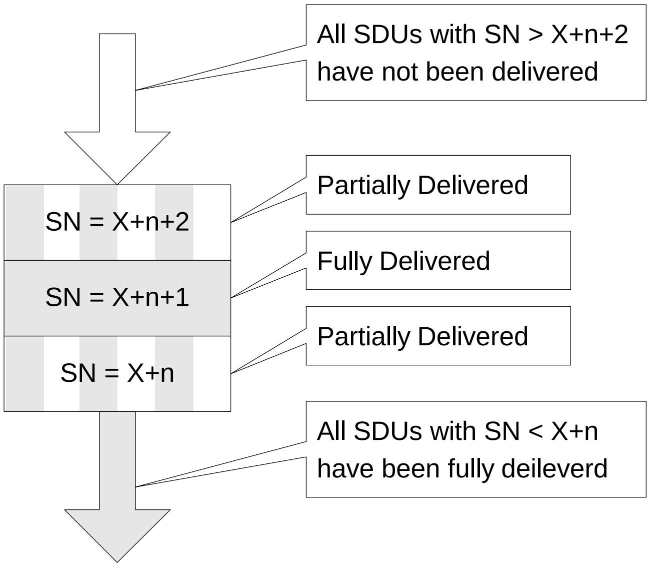

All SDUs with SN > X+n+2 have not been delivered
Partially Delivered
SN = X+n+2
Fully Delivered
SN = X+n+1
Partially Delivered
SN = X+n
All SDUs with SN < X+n have been fully deileverd

Figure 4-121 – Example of Transmission Queue in the Serving BS/ABS

In this case the Serving BS/ABS should report to the Target BS/ABS 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/AMS. Since the SDU with SN = X+n+1 has already been fully delivered, it will not be transmitted anew from the Target BS/ABS. 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/AMS should reset ARQ parameters after Re-Entry in the Target BS/ABS. This ARQ parameter reset will happen automatically after HO completion at the Target BS/ABS.

4.7.8.3.1.2 Buffering with Delivery on Demand Data Integrity Method

Per-SF Selective multi-unicasting explained in 4.7.8.3.1.1 provides for immediate availability of data in the Target BS/ABS 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/ABS/ASN-GWs.

Note also, that the Multi-Unicasting Data Integrity method implies buffering requirements at the Target BS/ABS(s). If additional backhaul capacity or buffer resources are not available at the Target BS/ABS(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 BS/ABSs (TBSs).

Buffering in Anchor ASN-GW follows the same rules as buffering in Target BS/ABS described in Sec. 4.7.8.3.1.1.

The Anchor ASN GW starts buffering immediately after receiving a Pre-Registration Request from any one of the Target BS/ABSs. 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/ABS, in turn, reports the SN to the Serving BS/ABS with HO Response, so the Serving BS/ABS knows from which part of data can be delivered to Target BS/ABS on demand. The Serving BS/ABS may then use this knowledge in order to deliver to MS/AMS the data that are not available in the Target.

The Serving BS/ABS delivers to the Target BS/ABS the information about the SDUs it has successfully delivered and about the SDUs that need to be delivered by the Target BS/ABS. The information is delivered with either HO Confirm message or Context Delivery Transaction in the way identical to that explained in Sec. 4.7.8.3.1.

4.7.8.3.1.3 BS Buffer Switching Method

This data integrity method requires data buffering at the Serving BS/ABS and forwarding the buffered data to the selected Target BS/ABS(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/ABS and, at the same time, optionally at the Target BS/ABS. Data packets buffered at the Serving BS/ABS SHALL be forwarded to the selected Target BS/ABS during the HO Action phase. The data buffering function SHALL be co-located with the handover decision making entity within the BS.

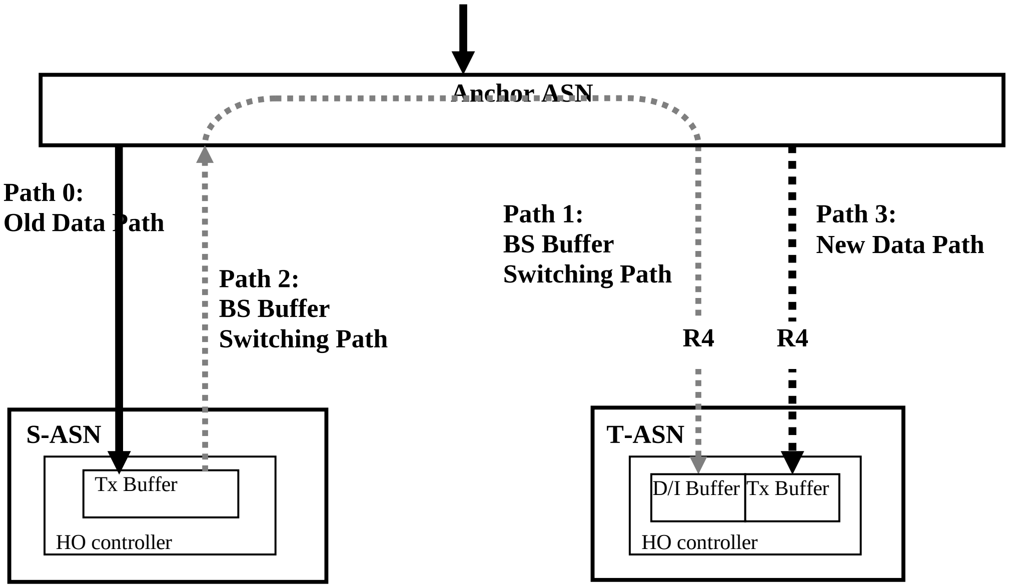
The data SHALL be forwarded to the Target BS/ABS(s) in one of two ways:

- 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

4.7.8.3.1.3.1 Data Delivery via Anchor ASN-GW



* Note: Dual buffers are shown at the Target BS/ABS for illustration purpose only.

Figure 4-122 – Data buffering and forwarding in BS Buffer Switching

4.7.8.3.1.3.1.1 Operations during HO Preparation phase

For this method, the ASN-GW SHALL forward data packets to the Serving BS/ABS as it does before the handover and the Serving BS/ABS SHALL transmit packets to MS/AMS via 802.16e air interface.

The Target BS/ABS(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/ABS. Completion of Buffer Switching path(s) between the Anchor and the Target BS/ABS(s) SHALL trigger the Anchor ASN-GW to start pre-registration of Buffer Switching path between the Anchor ASN-GW and the Serving BS/ABS - 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/ABS to forward the data traffic to the Target BS/ABS(s) via Anchor ASN-GW.

4.7.8.3.1.3.1.2 Operations during Action Phase

In the HO Action phase, upon receiving MOB_HO-IND message from the MS/AMS, the Serving BS/ABS SHALL stop transmitting packets for MS/AMS via the 802.16e air interface.

If the handover data integrity feature is supported per the BS buffer switching method, the Serving BS/ABS SHALL deliver the transmission status information of its buffered packets to the Target BS/ABS in a HO_Cnf message. The message SHALL include the SDU SN of the first SDU to be sent to the MS/AMS by the Target BS/ABS.

After receiving the HO_Cnf message, if the BS Buffer Switching paths (data paths 1, and 2 in the Figure 4-122) and New Data Path (data path 3 in the Figure 4-122) are not pre-registered, the Target BS/ABS SHALL initiate the Path Registration procedure to set up a Buffer Switching path (path 1) between the Anchor and the Target BS/ABS, 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/ABS 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/ABS 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.

Upon completion of the Buffer Switching path(s) between the Serving BS/ABS and the Anchor ASN-GW, the Serving BS/ABS SHALL start forwarding data packets which have been buffered at the Serving BS/ABS for air transmission at the Target BS/ABS.

If the Serving BS/ABS can determine that the MOB_HO-IND is lost in the air or receives MOB_HO-IND without BS ID, then the Serving BS/ABS MAY send _HO-Cnf with Unconfirmed indicator and forward buffered data packets to all candidates Target BS/ABS(s) which were indicated in the MOB_BSHO_RSP or MOB_BSHO_REQ.

If R4 data path(s) between the Anchor and the Target BS/ABS is pre-registered during the action phase, Target BS/ABS(s) MAY choose to activate the data transfer immediately. Hence, Anchor ASN-GW MAY start bi-casting of data packets (which are received by the Anchor ASN-GW via the R3 reference point) towards both the Serving and the Target BS/ABS. By default, Anchor ASN-GW SHALL send data packets towards the Serving BS/ABS.

4.7.8.3.1.3.1.3 Operations during Network re-entry.

Upon successful re-entry of MS/AMS at the Target BS/ABS, the Target ASN-GW SHALL send Path_Reg_Req message, which requests setup of New Data path (data path 3 in the Figure 4-122), and notifies the Anchor ASN-GW of the successful re-entry.

After receiving Path_Reg_Req from the Target BS/ABS, the Anchor ASN-GW SHALL stop forwarding data packets towards the Serving BS/ABS and switch data transmission to the Target BS/ABS. The SDU SN of the last transmitted data packet to the Serving BS/ABS SHALL be transmitted to the Target BS/ABS during the path registration between the Anchor and the Target BS/ABS (in Path Reg resp from Anchor ASN-GW). Timer $T_{Wait\_ServingBS\_SendEnd}$ is started After Target BS/ABS receives Path Reg RSP. After TWait_ServingBS_SendEnd is expired, the Target BS/ABS starts sending packets in the New Data buffer. Successful completion of the Path Registration procedure between the Anchor ASN-GW and the Target BS/ABS causes the Anchor ASN-GW to initiate the Data Path De-Registration procedure with the Serving ASN to remove the original data path (Path 0 in the figure). The SDU SN(sn) for the last transmitted packet by the Anchor ASN-GW is forwarded to the Serving BS/ABS in the data path deregistration request message so that the Serving BS/ABS can ensure that all the data packets are received before responding to the data de-registration request message from the anchor The Target BS/ABS starts buffering the data received from Anchor ASN-GW in Tx Buffer.

The SDU SN for the packet, last transmitted by the Anchor ASN-GW, can be forwarded to the Target BS/ABS in the data path registration response message. Target BS/ABS SHALL use this sequence number(sn) as well as the sequence number of the next packet destined for MS/AMS received in the HO Confirm message(sn') to ensure that all the data packets are received before the data path deregistration procedure for the Buffer Switching path(s). Upon receipt of the last packet, the–Target BS/ABS initiates the data path deregistration procedure for the Buffer Switching path(s) with the Anchor ASN for the buffer switching path(s). This automatically triggers the Anchor ASN-GW to initiate deregistration of the BS Buffer Switching path(s) with the Serving BS/ABS.

This step is important to ensure no data packets are lost during the data path de-registration procedure. In the Target BS/ABS, 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/ABS performs sequence number management to synchronize the buffers. If the Target BS/ABS 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/ABS SHALL trigger the Data Path De-registration procedure with the Anchor ASN-GW to remove the Buffer Switching path between the Anchor and the Target BS/ABS, which in turn causes the Anchor ASN-GW to initiate the data path de-registration of the Buffer Switching path between the Anchor ASN-GW and the Serving BS/ABS.

The Serving BS/ABS SHALL NOT flush its buffer until the data path de-registration procedure for the buffer switching path has been initiated. Upon receiving HO Complete message, Serving BS/ABS SHALL ensure that all the packets have been transferred to the Target BS/ABS prior to releasing the MAC context and data path(s).

The Target BS/ABS SHALL resume data transmission to MS/AMS by sending data packets received from the Serving BS/ABS first. In the Target BS/ABS, the data that was received from the Serving BS/ABS (D/I buffer) is transmitted to the MS/AMS 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/AMS. After successful transmission of packets buffered in the D/I buffer, the target BS/ABS SHALL flush the buffer.

4.7.8.3.1.3.1.4 Handover Call Flows

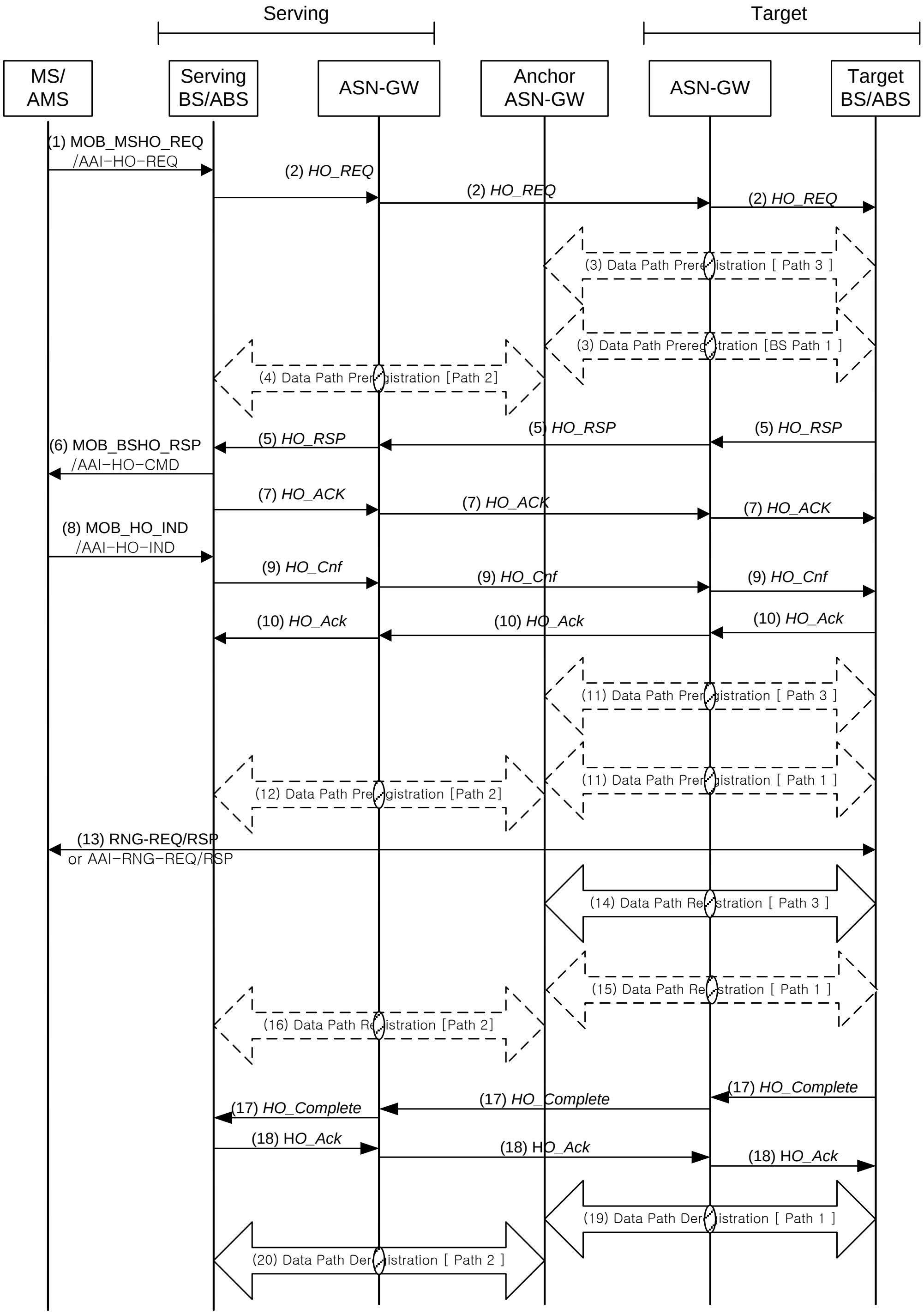

Serving
Target
MS/ AMS
Serving BS/ABS
ASN-GW
Anchor ASN-GW
ASN-GW
Target BS/ABS
(1) MOB_MSHO_REQ /AAI-HO-REQ
(2) HO_REQ
(2) HO_REQ
(2) HO_REQ
(3) Data Path Prere istration [Path 3]
(3) Data Path Prere tration [BS Path 1]
(4) Data Path Pre gistration [Path 2]
(5) HO_RSP
(5) HO_RSP
(5) HO_RSP
(6) MOB_BSHO_RSP /AAI-HO-CMD
(7) HO_ACK
(7) HO_ACK
(7) HO_ACK
(8) MOB_HO_IND /AAI-HO-IND
(9) HO_Cnf
(9) HO_Cnf
(9) HO_Cnf
(10) HO_Ack
(10) HO_Ack
(10) HO_Ack
(11) Data Path Pre gistration [Path 3]
(11) Data Path Pre gistration [Path 1]
(12) Data Path Pre gistration [Path 2]
(13) RNG-REQ/RSP or AAI-RNG-REQ/RSP
(14) Data Path Re stration [Path 3]
(15) Data Path Re stration [Path 1]
(16) Data Path R istration [Path 2]
(17) HO_Complete
(17) HO_Complete
(17) HO_Complete
(18) HO_Ack
(18) HO_Ack
(18) HO_Ack
(19) Data Path Der istration [Path 1]
(20) Data Path Der istration [Path 2]

Figure 4-123 – Data Delivery via Anchor ASN-GW

STEP 1

The MS/AMS initiates a handover by sending a MOB_MSHO-REQ/AAI-HO-REQ message to the serving BS/ABS which includes one or more potential target BS/ABS's.

STEP 2

The serving BS/ABS sends an *HO_Req* message to one or more potential target BS/ABS'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/ABS 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**).

Note: BS Buffer Switching data path 1 and normal data path 3 should be established independently.

STEP 4

Optional: Upon receipt of the data path pre-registration request from the target BS/ABS to its data integrity buffer (path 1), the Anchor ASN-GW initiates a data path from the Serving BS/ABS to the Anchor ASN-GW (path 2) to complete a buffer switching path from the serving BS/ABS to the target BS/ABS 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/ABS(s) sends a *HO_Rsp* message to the serving BS/ABS to acknowledge the handover request and starts $T_{R6\_HO\_Rsp}$. Upon receipt of the *HO_Rsp* message, the serving BS/ABS stops timer $T_{R6\_HO\_Req}$.

STEP 6

The Serving BS/ABS sends a MOB_BSHO-RSP/AAI-HO-CMD message to the MS/AMS.

STEP 7

The serving BS/ABS sends a *HO_Ack* message to the target BS/ABS(s). Upon receipt of the *HO_Ack* message, the Target BS/ABS(s) stops timer $T_{R6\_HO\_Rsp.}$

STEP 8

The MS/AMS sends a MOB_HO-IND message to the serving BS/ABS to notify it of its intent to handover to a target BS/ABS as proposed by the serving BS/ABS in the handover preparation phase.

STEP 9

Upon reception of the MOB_HO-IND message, the Serving BS/ABS sends a *HO_Cnf* message to the Target BS/ABS and starts timer $T_{R6\_HO\_Conf}$.

STEP 10

The Target BS/ABS sends a *HO_Ack* message to the Serving BS/ABS. Upon receipt of the *HO_Ack* message, the Serving BS/ABS stops timer $T_{R6\_HO\_Conf}$. If data path pre-registration occurred in steps 3 and 4, the serving BS/ABS begins transferring data packets to the target BS/ABS via the Anchor ASN-GW (path 2 and path 1) starting with the first packet to be transmitted to the MS/AMS. The target BS/ABS 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/ABS 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/ABS for a data path from the anchor ASN-GW and the target BS/ABS's data integrity buffer (path 1), the anchor ASN-GW initiates registration of a data path from the serving BS/ABS to the anchor ASN-GW (path 2) to complete a buffer switching path from the serving BS/ABS to the target BS/ABS (see section **4.12.1**). The *data delivery trigger* TLV in the path pre-registration request message is set to 1. The serving BS/ABS begins transferring data packets received from the anchor ASN-GW to the target BS/ABS via the anchor ASN-GW (path 2 and path 1) starting with the first packet to be transmitted to the MS/AMS. The target BS/ABS buffers the packets in it data integrity buffer.

STEP 13

The MS/AMS initiates network re-entry at the Target BS/ABS. The target BS/ABS begins transmitting data packets to the MS/AMS starting with data packets buffered in its data integrity buffer.

STEP 14

The Anchor ASN-GW and Target BS/ABS 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/ABS 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/ABS for a data path from the anchor ASN-GW and the target BS/ABS's data integrity buffer (path 1), the anchor ASN-GW initiates registration of a data path from the serving BS/ABS to the anchor ASN-GW (path 2) to complete a buffer switching path from the serving BS/ABS to the target BS/ABS (see section **4.12.1**). The *data delivery trigger* TLV in the path pre-registration request message is set to 1. The serving BS/ABS begins transferring data packets received from the anchor ASN-GW to the target BS/ABS via the anchor ASN-GW (path 2 and path 1) starting with the first packet to be transmitted to the MS/AMS. The target BS/ABS buffers the packets in it data integrity buffer.

STEP 17

The target BS/ABS sends a *HO_Complete* message to notify the serving BS/ABS that the MS/AMS was successfully acquired. Upon receipt of the *HO_Complete* message, the serving BS/ABS releases the MS context and starts timer $T_{R6\_HO\_Comp}$.

STEP 18

The serving BS/ABS sends a HO_Ack message to the Target BS/ABS. After receipt of the HO_Complete message and the buffer switching paths are deregistered, the serving BS/ABS releases the MS context. Upon receipt of the HO_Ack message, the Target BS/ABS stops timer TR6_HO_Comp.

STEP 19

The target BS/ABS 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/AMS by invoking the Data Path De-Registration procedure (see section 4.12).

STEP 20

Upon receipt of a request to deregister the data path between the anchor ASN-GW and the target BS/ABS'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/ABS (path 2) by invoking the Data Path De-Registration procedure (see section 4.12).

Note: Serving BS/ABS may initiate de-registration of data path 0 at any time after step 16 and/or expiration of the resource retain timer.

4.7.8.3.1.3.2 Direct Data Delivery Method

In this method the buffered data is delivered to the Target BS/ABS directly using R8 data path between the BSs.

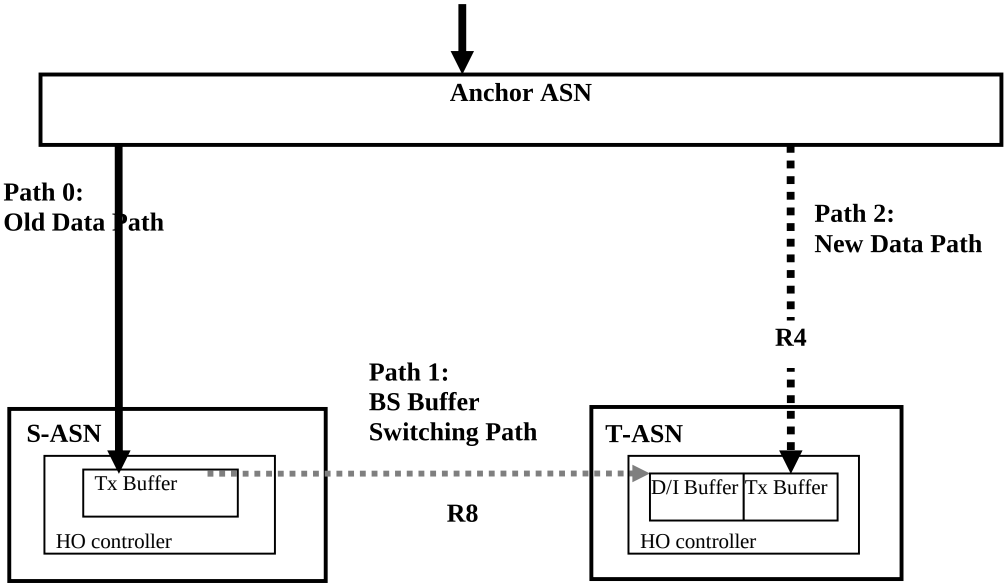


Figure 4-124 – Data buffering at the Serving BS/ABS and forwarding via R8

*Note: Reference to D/I buffer here is for illustration purpose.

4.7.8.3.1.3.2.1 Operations during Preparation Phase

The Target BS/ABS(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/ABS(s) and the Anchor ASN-GW to avoid multi uni-casting to the target. Capability negotiation for R8 data path setup between Serving BS/ABS and Target BS/ABS is shown in section 4.7.8.5. For the purpose of setting a direct data path (path 1) between the Serving BS/ABS and the Target BS/ABS, GRE Keys for R8 data path may be exchanged between the Target BS/ABS and the Serving BS/ABS via R8 HO Request / HO response. Alternatively, the serving BS/ABS and target BS/ABS may setup a direct data path (path1) by exchanging GRE keys for R8 data path using path pre-registration procedure. 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.

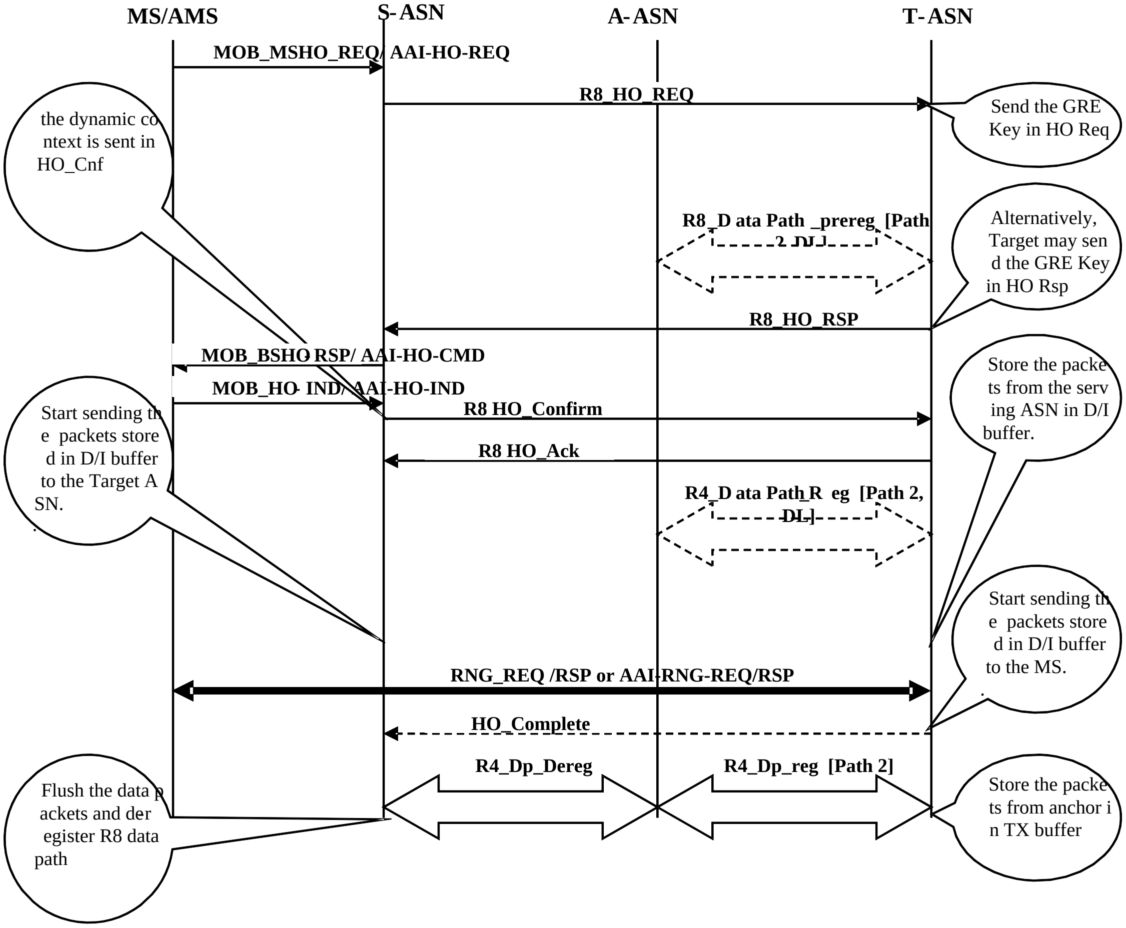

MS/AMS
S-ASN
A-ASN
T-ASN
MOB_MSHO_REQ/ AAI-HO-REQ
R8_HO_REQ
the dynamic context is sent in HO_Cnf
Send the GRE Key in HO Req
R8_D ata Path _prereg [Path 2 DL]
Alternatively, Target may send the GRE Key in HO Rsp
R8_HO_RSP
MOB_BSHO RSP/ AAI-HO-CMD
MOB_HO IND/ AAI-HO-IND
Store the packets from the serving ASN in D/I buffer.
R8 HO_Confirm
Start sending the packets stored in D/I buffer to the Target ASN.
R8 HO_Ack
R4_D ata Path_R eg [Path 2, DL]
Start sending the packets stored in D/I buffer to the MS.
RNG_REQ /RSP or AAI-RNG-REQ/RSP
HO_Complete
R4_Dp_Dereg
R4_Dp_reg [Path 2]
Flush the data packets and deregister R8 data path
Store the packets from anchor in TX buffer

Figure 4-125 – Data integrity procedures for Direct data delivery method

4.7.8.3.1.3.2.2 Operations during Action Phase

Upon receipt of MOB_HO-IND message with the selected Target BS/ABS ID from the MS/AMS, the Serving BS/ABS sends HO confirm to the Target BS/ABS. If the data path between the Target BS/ABS and the Anchor ASN-GW is not already established, the Target BS/ABS SHALL pre-register new data path (path 2). Similarly, if the direct data path (BS buffer switching path) to the Serving BS/ABS is not already established, Target BS/ABS SHALL register an R8 data path with the serving BS/ABS at this time. HO confirm message MAY be used as a trigger for the data forwarding from the Serving BS/ABS over the R8 data path between the Serving and Target BS/ABS. The SDU SN of the next packet destined for MS/AMS is forwarded to the Target BS/ABS in the HO Confirm message initiated by the Serving BS/ABS. Upon activation of data path, Serving BS/ABS initiates the data transfer to the Target BS/ABS via the GRE tunnel or it may choose to buffer the packets. This is based on the local policies. Target BS/ABS buffers these packets received over R8 in D/I buffer.

Optionally, if the Serving BS/ABS 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/ABS sends HO confirm with un-confirm indication and may initiate data transfer to all candidate Target BS/ABS(s) which were indicated in the MOB_BSHO-RSP/AAI-HO-CMD or MOB_BSHO-REQ/AAI-HO-CMD.

Optionally, if data path(s) (Path 2) between the Anchor ASN-GW and the Target BS/ABS is pre-registered during the action phase, the Target BS/ABS(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/ABS(s).

4.7.8.3.1.3.2.3 Operations during Network Entry Phase

Upon successful completion of network re-entry of the MS/AMS, Target BS/ABS 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/AMS, and starts forwarding the data packets from D/I buffer to the MS/AMS. In parallel, Target BS/ABS also initiates data path registration procedure to the Anchor ASN-GW. Anchor ASN-GW switches downlink traffic from the Serving BS/ABS to the Target BS/ABS and initiates data path deregistration procedure to the Serving BS/ABS. The SDU SN(sn) for the last transmitted packet by the Anchor ASN-GW is forwarded to the Serving BS/ABS in the data path deregistration request message so that the Serving BS/ABS 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/ABS starts buffering the data received from Anchor ASN-GW in Tx Buffer.

The Serving BS/ABS completes the transfer of all the data in its resource retention buffer to the Target BS/ABS. If HO complete is received, Serving BS/ABS SHALL ensure that all the packets have been transferred to the Target BS/ABS 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/ABS.

The SDU SN (sn) for the last transmitted packet by the Anchor ASN-GW can be forwarded to the Target BS/ABS in the data path registration response message. Target BS/ABS SHALL use this sequence number(SN) as well as the sequence number of the first unsent packet destined for the MS/AMS 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/ABS. Upon receipt of the last packet, the-Target BS/ABS initiates the data path deregistration procedure for the Buffer Switching path(s) with the Serving BS/ABS.

This step is important to ensure no data packets are lost during the data path de-registration procedure. In the Target BS/ABS, 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/ABS 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/ABS SHALL ensure the Data Path De-registration procedure with the Serving BS/ABS to remove the Buffer Switching path between the Serving and the Target BS/ABS, which in turn causes the serving BS/ABS to initiate the data path de-registration of the old data path between the Anchor ASN-GW and the Serving BS/ABS.

The Serving BS/ABS 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/ABS SHALL ensure that all the packets have been transferred to the Target BS/ABS prior to releasing the MAC context and data path(s).

In the Target BS/ABS, the data that was received from the Serving BS/ABS (D/I Buffer) is transmitted to the MS/AMS 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/AMS.

[Note]: Refer to Stage3 ASN Anchored Mobility section for details of releasing MAC context.

4.7.8.3.2 Uplink Data Integrity

Uplink Data Integrity support is required when ARQ synchronization is supported. It is only required that the Serving BS/ABS delivers to the Target BS/ABS the SN from which the Target BS/ABS should start numbering its uplink SDUs.

If the Serving BS/ABS has some uncompleted SDUs received from MS/AMS it SHALL discard them after De-Registration of Data Path with the Anchor ASN-GW.

4.7.8.3.3 Auxiliary Use of SDU SN Report

The Serving and Target BS/ABSs and the MS/AMS may perform MS-Assisted coordination of DL transmission during handover as described in *802.16e section 6.3.22.2.8*. The Target BS/ABS may signal to the MS/AMS on the intention to apply this procedure by using Bit #11 of 'HO Process Optimization/Reentry Process Optimization' bitmask in the RNG-RSP message. The Serving BS/ABS may transmit 'HO Process Optimization/Reentry Process Optimization' bitmask in the MOB_BSHO-RSP/AAI-HO-CMD or MOB_BSHO-REQ/AAI-HO-CMD messages.

For ARQ enabled connections, the MS/AMS may report to the Target BS/ABS 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/AMS takes precedence over the ARQ Sync information received from the Serving BS/ABS in case of mismatch.

For ARQ disabled connections, the MS/AMS may report to the Target BS/ABS 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/AMS and the BS is described in *892.16e section 6.3.22.2.8*. The Serving BS/ABS should make sure that SDU SN in the MS/AMS is equal to the reminder of integer division by 255 of the corresponding SDU SN in the GRE Header. The Target BS/ABS should make sure that SDU numbering in the MS/AMS continues after handover.

4.7.8.3.4 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 4.7.8.

The Table 4-108 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 4-108 –Info in HO_Req

IE	Reference	M/O	Notes
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 4-109 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 4-109 – 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/AMS 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/ABS.
>>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 4-110 specifies placement and meaning of the SDU Info in HO Confirm from the Serving BS/ABS to the Target BS/ABS.

Table 4-110 – SDU Info in HO_Cnf From Serving BS/ABS to Target BS/ABS

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	O	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/ABS. 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/ABS may expect to receive from the MS/AMS.
>>>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 4-111 – SDU SN in Path_De-Reg Req from Serving ASN GW to Serving BS/ABS, Anchor ASN-GW to Serving BS/ABS

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	O	SFID associated with the Service Flow. This TLV SHALL be included if SDU 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 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/AMS.
>>>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.

4.7.8.4 Data Integrity with ARQ Synchronization

Data Integrity procedures may involve ARQ State Synchronization between the Serving BS/ABS and Target BS/ABS. ARQ State Synchronization is optional and is negotiated between the Serving and Target BS/ABS. It is added on the top of related basic Data Integrity procedures specified in 4.7.8.3.

If ARQ State is synchronized between Serving BS/ABS and Target BS/ABS for ARQ enabled Service Flows the MS/AMS and the Target (New Serving) BS resume data transmission from the very point it stopped between the MS/AMS and Old Serving ASN when handover happened.

If ARQ State Synchronization is agreed between the Serving and Target BS/ABS, then the MS/AMS SHALL be notified of expected ARQ Synchronization by setting the “Full Service and Operational State Transfer” bit in the “HO Process Optimization/Reentry Process Optimization” bitmask that is delivered to the MS/AMS over the air.

The Target BS/ABS transmits “HO Process Optimization/Reentry Process Optimization” bitmask in RNG-RSP. The Serving BS/ABS (Serving BS/ABS) transmits ‘HO Process Optimization/Reentry Process Optimization’ bitmask in MOB_BSHO-RSP/AAI-HO-CMD or MOB_BSHO-REQ/AAI-HO-CMD. 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.

4.7.8.4.1 Synchronization of ARQ State

4.7.8.4.1.1 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 4-112 lists these parameters.

Table 4-112 –

Parameter	Description
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.
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 *sections 6.3.4.6.2 and 6.3.4.6.3 in IEEE 802.16e standard*.
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 section 6.3.4.6.3* in *IEEE 802.16e standard)*.
ARQ_BLOCK_SIZE	The length (in octets) used for partitioning an SDU into a sequence of Blocks prior to transmission (see *section 6.3.4.1* in *IEEE 802.16e standard*).

The aforementioned parameters are communicated between BS and MS/AMS 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 BS/ABSs during the HO Preparation Phase.

4.7.8.4.1.2 Synchronizing Downlink ARQ State after handover

From IEEE 802.16e perspective synchronization of the Downlink ARQ State means the following:

If MS/AMS received DISCARD message from the Serving BS/ABS but couldn't reply with acknowledgement, the MS/AMS SHALL send the acknowledgement to the Target BS/ABS. The MS/AMS may send the acknowledgements immediately after handover completion or may postpone it depending on the state of its internal timers.

The Target BS/ABS SHALL never transmit the ARQ blocks up to the one specified in the last DISCARD message from the Serving BS/ABS. The Target BS/ABS may re-transmit the DISCARD message (first transmitted by the Serving BS/ABS) immediately after handover or it may postpone the retransmission up until ARQ_RETRY_TIMEOUT after completion of handovers. If the Target BS/ABS 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/AMS had successfully received an ARQ block from the Serving BS/ABS but couldn't reply send the acknowledgement to the Serving BS/ABS, the MS/AMS SHALL send the acknowledgement to the Target BS/ABS. The MS/AMS SHALL send the acknowledgements immediately after HO completion or may postpone it depending on the state of its internal timers.

If the Serving BS/ABS has transmitted an ARQ block to the MS/AMS, but it was not acknowledged by the MS/AMS, the Target BS/ABS 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/AMS.

If the Serving BS/ABS has transmitted an ARQ block to the MS/AMS, and the MS/AMS acknowledged it, the Target BS/ABS 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/ABS (in the Serving and Target BS/ABSs 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/ABS, which may occur prior to MS/AMS leaving, is shown on the Figure 4-126. The transmission buffer in the Serving BS/ABS 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.

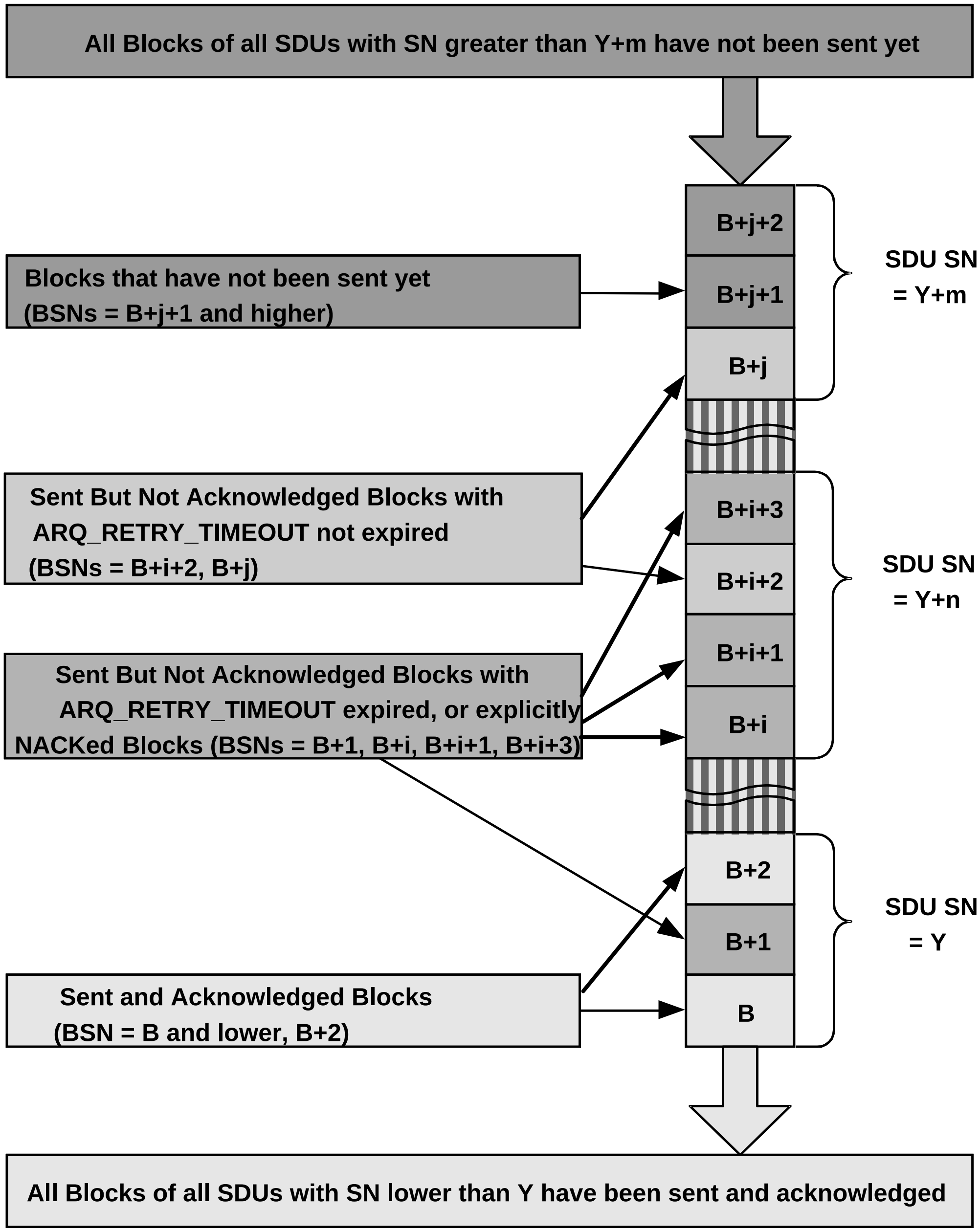

All Blocks of all SDUs with SN greater than Y+m have not been sent yet
B+j+2
B+j+1
B+j
SDU SN
= Y+m
Blocks that have not been sent yet
(BSNs = B+j+1 and higher)
Sent But Not Acknowledged Blocks with
ARQ_RETRY_TIMEOUT not expired
(BSNs = B+i+2, B+j)
B+i+3
B+i+2
B+i+1
B+i
SDU SN
= Y+n
Sent But Not Acknowledged Blocks with
ARQ_RETRY_TIMEOUT expired, or explicitly
NACKed Blocks (BSNs = B+1, B+i, B+i+1, B+i+3)
B+2
B+1
B
SDU SN
= Y
Sent and Acknowledged Blocks
(BSN = B and lower, B+2)
All Blocks of all SDUs with SN lower than Y have been sent and acknowledged

Figure 4-126 – Example of per-SF Downlink Transmission Queue in Serving BS/ABS

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 4-126 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 4-126 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 4-126 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.

4.7.8.4.1.3 Synchronizing Uplink ARQ State after handover

From IEEE 802.16e perspective synchronization of the Downlink ARQ State means the following:

The MS/AMS 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/ABS has successfully received an ARQ block from the MS/AMS, but couldn't reply with acknowledgement to the MS/AMS, the Target BS/ABS SHALL send the acknowledgement to the MS/AMS. The Target BS/ABS may send the acknowledgements immediately after HO completion or may postpone it depending on the state of its internal timers.

If the MS/AMS has been transmitted an ARQ block to the Serving BS/ABS, but did not receive acknowledgement from the Serving BS/ABS, the MS/AMS SHALL start retransmitting it to the Target BS/ABS. 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/AMS.

If the MS/AMS has transmitted an ARQ block to the Serving BS/ABS, and received acknowledgement from the Serving BS/ABS, the MS/AMS SHALL NOT transmit it again to the Target BS/ABS 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/ABS, which may occur prior to MS/AMS leaving, is shown on the Figure 4-127. The reception buffer in the Serving BS/ABS 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.

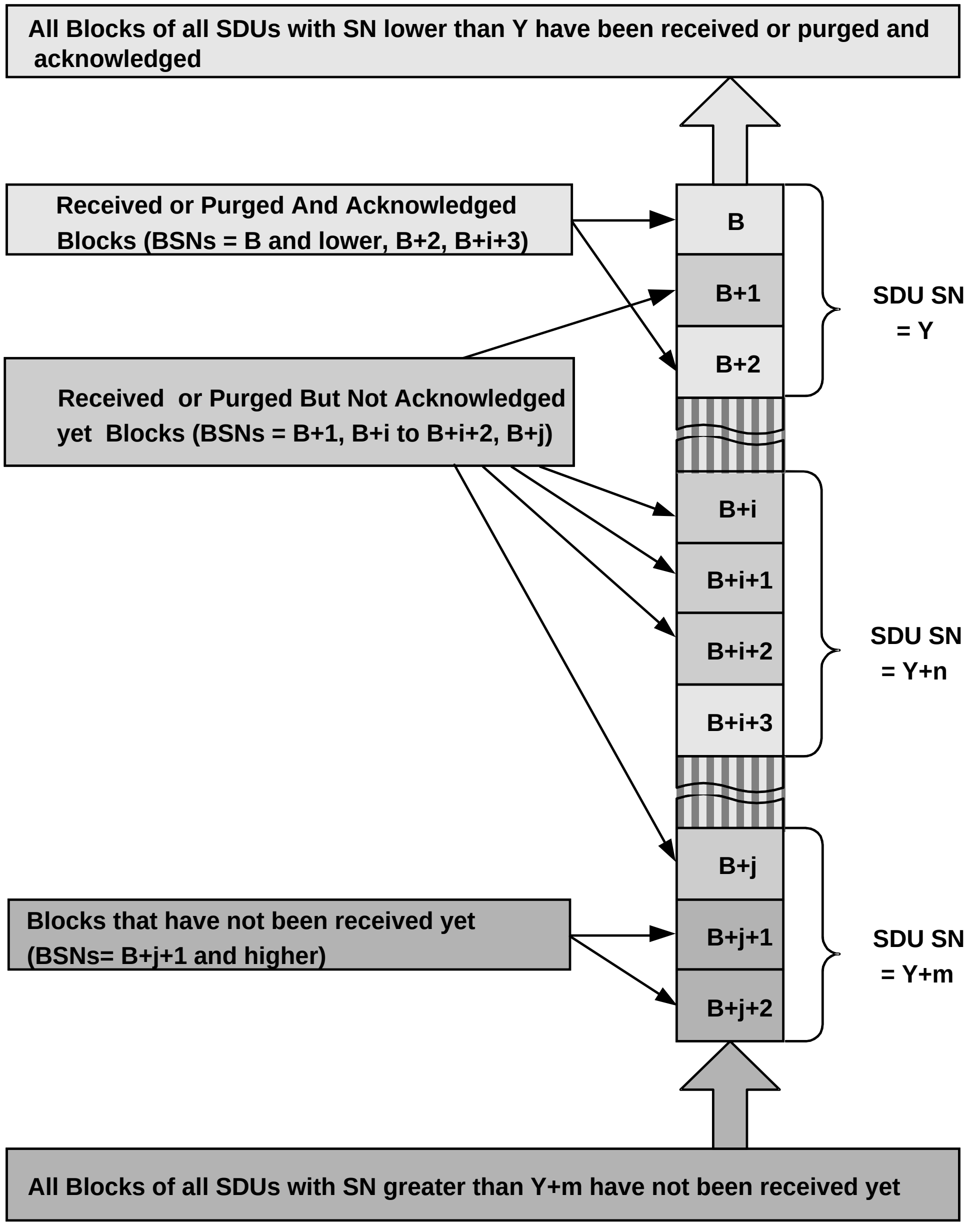

All Blocks of all SDUs with SN lower than Y have been received or purged and acknowledged
Received or Purged And Acknowledged Blocks (BSNs = B and lower, B+2, B+i+3)
Received or Purged But Not Acknowledged yet Blocks (BSNs = B+1, B+i to B+i+2, B+j)
Blocks that have not been received yet (BSNs= B+j+1 and higher)
All Blocks of all SDUs with SN greater than Y+m have not been received yet
B
B+1
B+2
B+i
B+i+1
B+i+2
B+i+3
B+j
B+j+1
B+j+2
SDU SN = Y
SDU SN = Y+n
SDU SN = Y+m

Figure 4-127 – Example of per-SF Uplink Reception Queue in Serving BS/ABS

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 4-127 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 4-127 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 4-127 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/AMS.

4.7.8.4.2 Downlink Data Integrity Methods

This section describes each specific method that can be applied for downlink data integrity with ARQ synchronization support during handover.

4.7.8.4.2.1 BS Buffer Switching with ARQ State And Buffer Synchronization

This method acts on top of the BS Buffer Switching method described in Sectection 4.7.8.3.1.3. This method employs an appropriate way for synchronization of ARQ state between the Serving and Target BS/ABS. The Serving BS/ABS 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/ABS. The Serving BS/ABS SHALL forward those ARQ blocks to the Target BS/ABS before it forwards IP packets waiting for transmission to MS/AMS in its buffer. Those ARQ blocks which are forwarded between BSs SHALL be grouped into small Data Integrity packets as illustrated in the Figure 4-128 – Data Integrity Packets to Forward ARQ Blocks (Example)

. 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. The packet length carries the length of the payload of DI packet and does not include the length of the mini-header.

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 with discontinuous BSN for the ARQ blocks, a Data Integrity Mini-header SHALL be inserted between them.

For detailed information on Data Integrity Mini-header, refer to Table 4-113.

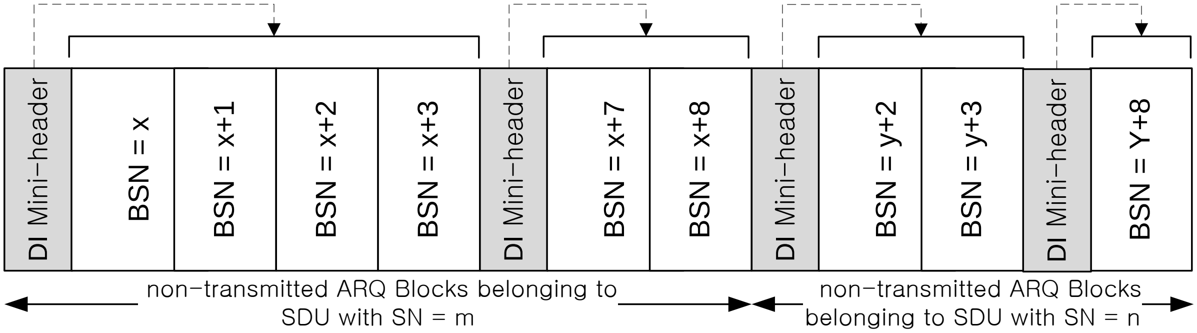


Figure 4-128 – Data Integrity Packets to Forward ARQ Blocks (Example)

Note: In the example above, the ARQ Blocks with block sequence numbers x+4, x+5, x+6 belong to SDU = m and y, y+1, y+4, y+5, y+6, y+7 belong to SDU = n had been acknowledged while the MS/AMS was served by the Serving ASN. Hence these are not included in the forwarded packets and are not shown in the figure.

Table 4-113 – 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. The packet length carries the length of the payload of DI packet and does not include the length of the mini-header.
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/ABS 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 4-114 in the section 4.7.8.4.5.

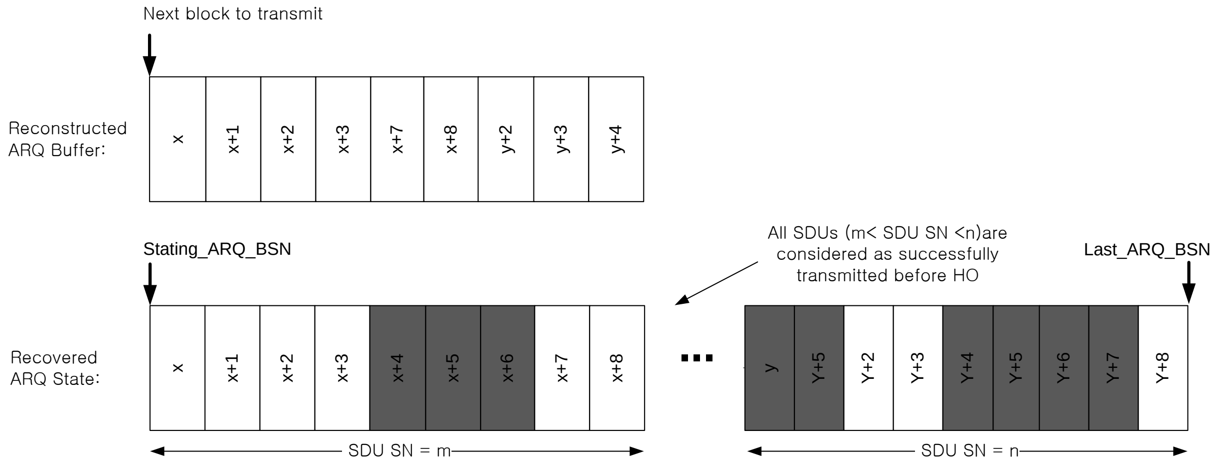


Figure 4-129 – Reconstruction of ARQ Buffers and State Machines at Target BS/ABS (Example)

*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/AMS resided in the Serving ASN, and are not sent by the Serving BS/ABS. Those blocks are pictured as black boxes in the forwarding packets in the figure.

4.7.8.4.3 Uplink Data Integrity Methods

This section describes each specific method that can be applied for uplink data integrity with ARQ synchronization support during handover.

4.7.8.4.3.1 SDU Reassembly Method

If ARQ State Synchronization is agreed between the Target and Serving BS/ABSs, then Uplink SDU Reassembly (either at the Data Path Anchor or at the Target BS/ABS) might be negotiated among the Target BS/ABS, Serving BS/ABS 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 4.7.8.4.1.3 is that parts of the uplink SDUs can be received in the Serving BS/ABS while the other parts can be received in the finally selected Target BS/ABS.

For example, consider delivery of the SDU with SN = Y+n on the Figure 4-127. 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/ABS.

As it has been mentioned in 4.7.8.4.1.3, if the MS/AMS 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).

4.7.8.4.3.1.1 Uplink SDU Reassembly at Anchor ASN-GW

If the SDU Reassembly at the Anchor ASN-GW is used, the Serving BS/ABS 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 4-127) while the Target BS/ABS 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 4-127). 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 4-130.

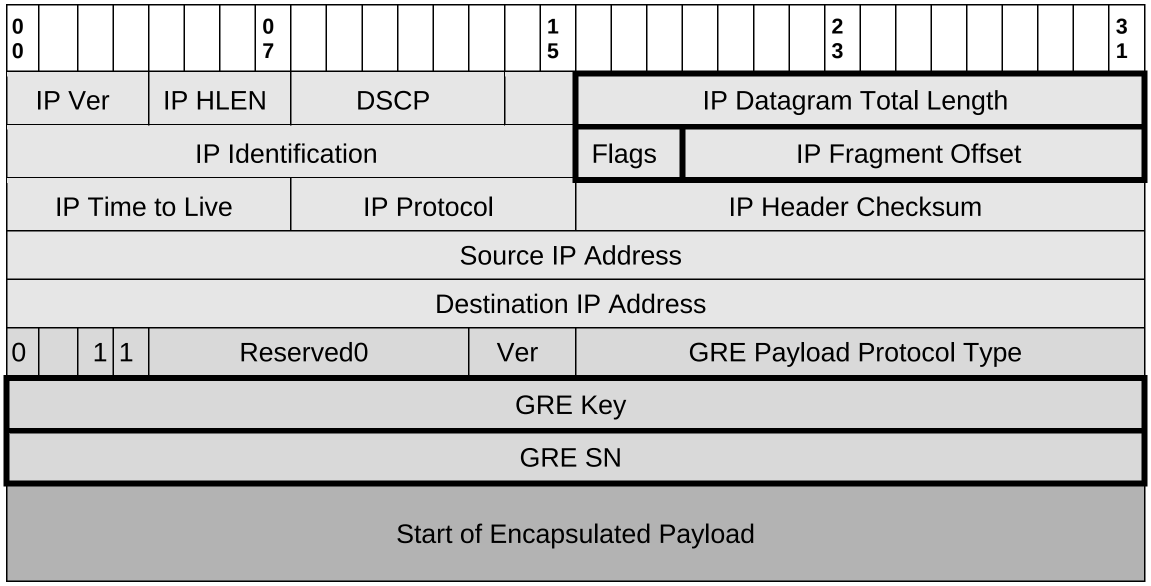


Figure 4-130 – Fields of the Outer Header Relevant for Uplink SDU Reassembly at Anchor ASN-GW

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 4-131 shows an example of such a tree.

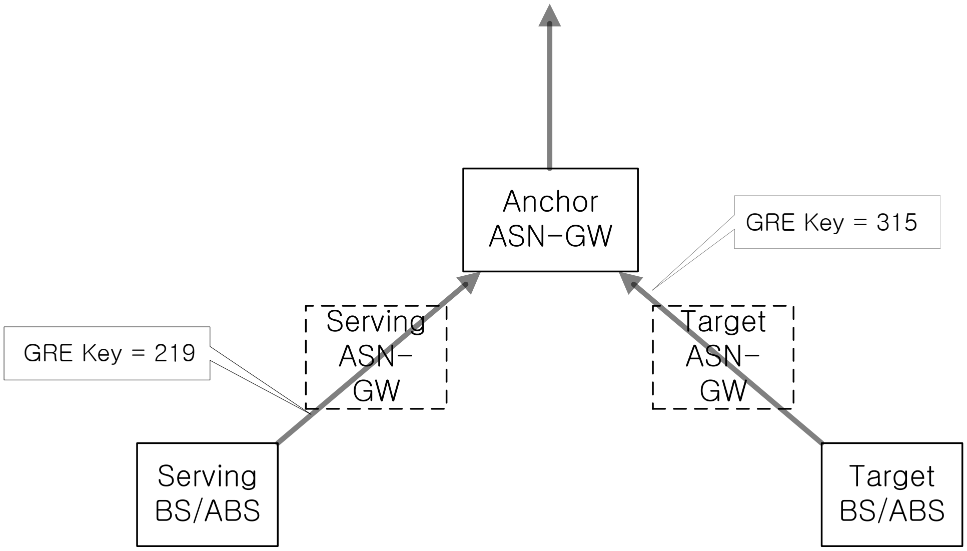


Figure 4-131 – Uplink Data Path Tree

Assume the SDU with SN = Y+n on the Figure 4-127 is to be delivered to the Anchor ASN-GW from the Serving BS/ABS and Target BS/ABS. The corresponding Data Path Tree is shown on the Figure 4-131.

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.

The two fragments sent from the Serving BS/ABS appear on the Figure 4-132 and Figure 4-133.

The first fragment, sent from the Serving BS (Figure 4-131) and corresponding to the Blocks with BSNs = B+i and B+i+1, appears on the Figure 4-132.

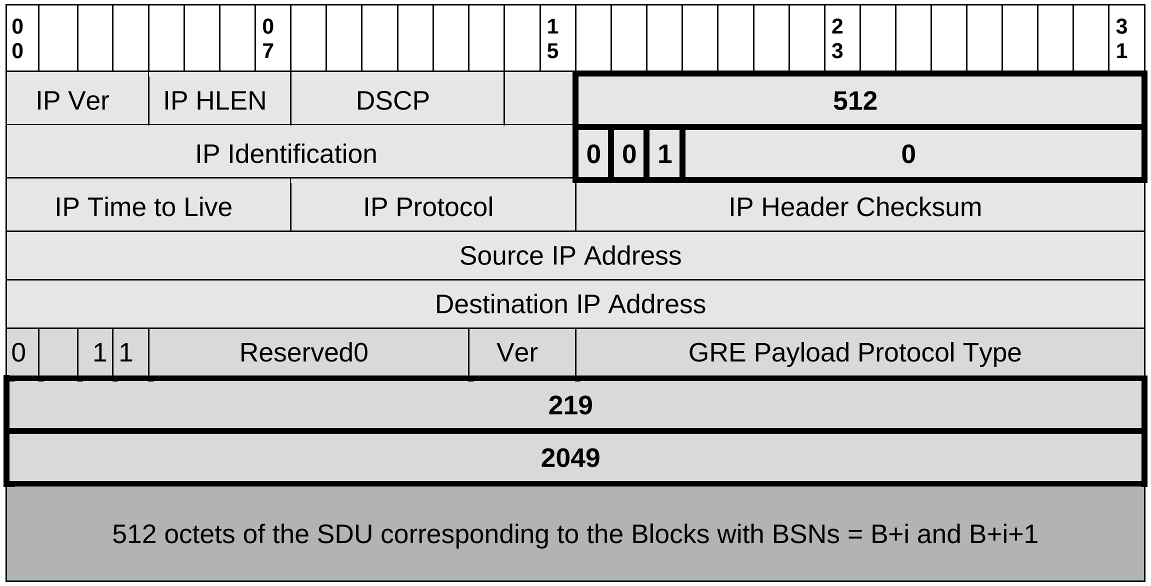


Figure 4-132 – First Fragment Sent from the SBS

The second fragment sent from the Serving BS/ABS and corresponding to the Block with BSN = B+i+3, appears on the Figure 4-133.

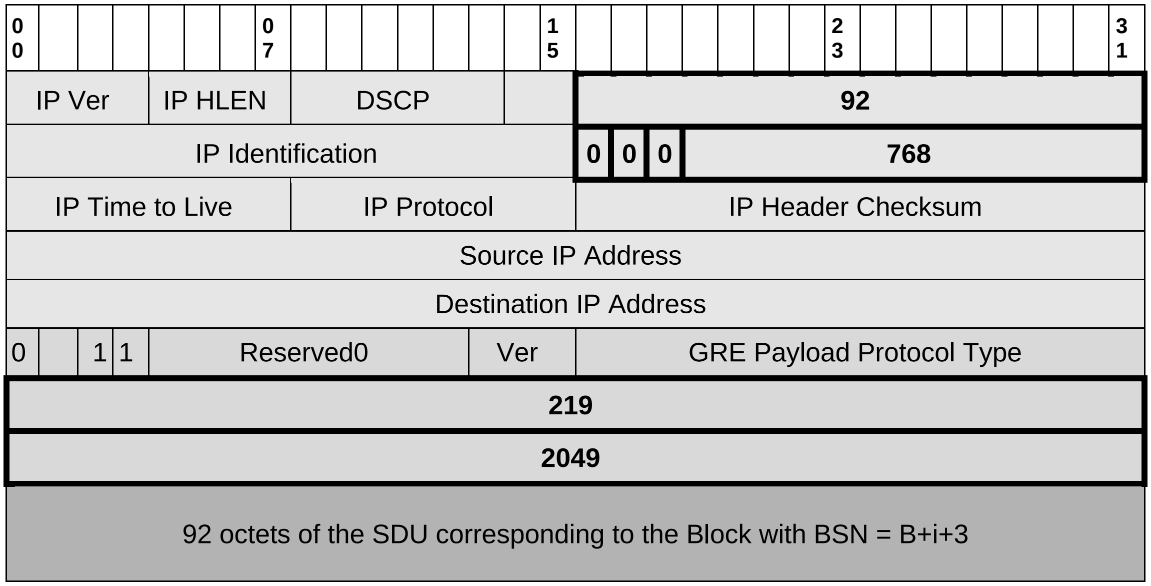


Figure 4-133 – Second Fragment Sent from the SBS

The fragment sent from the Target BS/ABS and corresponding to the Block with BSN = B+i+2 appears on the Figure 4-134.

<table>
<tr><td>00</td><td colspan="6"></td><td>07</td><td colspan="7"></td><td>15</td><td colspan="7"></td><td>23</td><td colspan="7"></td><td>31</td></tr>
<tr><td colspan="4">IP Ver</td><td colspan="4">IP HLEN</td><td colspan="6">DSCP</td><td colspan="2"></td><td colspan="16"><b>256</b></td></tr>
<tr><td colspan="16">IP Identification</td><td><b>0</b></td><td><b>0</b></td><td><b>1</b></td><td colspan="13"><b>512</b></td></tr>
<tr><td colspan="8">IP Time to Live</td><td colspan="8">IP Protocol</td><td colspan="16">IP Header Checksum</td></tr>
<tr><td colspan="32">Source IP Address</td></tr>
<tr><td colspan="32">Destination IP Address</td></tr>
<tr><td>0</td><td></td><td>1</td><td>1</td><td colspan="9">Reserved0</td><td colspan="3">Ver</td><td colspan="16">GRE Payload Protocol Type</td></tr>
<tr><td colspan="32"><b>315</b></td></tr>
<tr><td colspan="32"><b>2049</b></td></tr>
<tr><td colspan="32">256 octets of the SDU corresponding to the Block with BSN = B+i+2</td></tr>
</table>

Figure 4-134 – Fragment Sent from the TBS

The fragments produced according to the method described have different IP identification fields even if the source IP Address is the same. This feature differentiates them from ordinary IP fragments. This circumstance allows the described functionality to coexist with standard IETF IP fragmentation. The entity, which reassembles the fragments in the Anchor ASN-GW, can distinguish between the types of fragmentation and if two fragments have the same identification fields and the same source IP addresses then they should be reassembled as described in the *RFC 791.*

4.7.8.4.3.1.2 Uplink SDU Reassembly at Target BS/ABS (BS Buffer Switching with ARQ State And Buffer Synchronization)

This method is the same as the BS Buffer Switching with ARQ State and Buffer Synchronization described in Sec. 4.7.8.4.2.1, except that this is for uplink data traffic.

If the SDU Reassembly at the Target BS/ABS is used, the Serving BS/ABS will send 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+3 in the Figure 4-127) to the Target BS/ABS through the BS Buffer Switching data path, to be reassembled at the Target BS/ABS with the rests of the SDUs which can be received at the Target BS/ABS (e.g., fragments which consists of the ARQ Block with BSN = B+i+2 in the Figure 4-127). The reassembly of these ARQ Blocks at the Target BS/ABS is the same as the normal reassembly process at the Target ASN.

If the functionality is not agreed between the involved entities the uncompleted SDUs will be dropped by the Serving ASN after HO completion.

To forward the leftover uplink fragments (ARQ Blocks) of SDUs to the Target BS/ABS, the Serving BS/ABS SHALL group ARQ Blocks into small Data Integrity packets as illustrated in the Figure 4-128 in Sec. 4.7.8.4.2.1. 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 belong differ, a Data Integrity Mini-header SHALL be inserted between those groups (e.g., for ARQ Blocks of SDU "Y+n" in the Figure 4-127, the following Data Integrity packet SHALL be forwarded between BSs.)

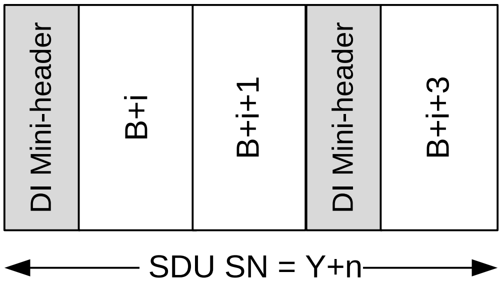


Figure 4-135 – Data Integrity Packets to Forward ARQ Blocks (Example)

4.7.8.4.4 Auxiliary Use of SDU SN Report

The Serving and Target BS/ABSs and the MS/AMS may perform MS-Assisted coordination of DL transmission during handover as described in *802.16e section 6.3.22.2.8*. The Target BS/ABS may signal to the MS/AMS on the intention to apply this procedure by using Bit #11 of 'HO Process Optimization/Reentry Process Optimization' bitmask in the RNG-RSP message. The Serving BS/ABS may transmit 'HO Process Optimization/Reentry Process Optimization' bitmask in the MOB_BSHO-RSP/AAI-HO-CMD or MOB_BSHO-REQ/AAI-HO-CMD messages.

For ARQ enabled connections, the MS/AMS may report to the Target BS/ABS 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/AMS takes precedence over the ARQ Sync information received from the Serving ASN in case of mismatch.

4.7.8.4.5 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 4.7.8.5.

Since ARQ Synchronization is added on top of the basic Data Integrity functionality described in 4.7.8.3 new Informational Elements are added to those already described in 4.7.8.3.4.

HO Request delivers to the Target BS/ABS the ARQ State Machine parameters discussed in 4.7.8.4.1. The exact formats of the TLVs are specified in section 5.

Additional content of HO_Cnf on top of baseline is shown here.

Table 4-114 – Additions HO_Cnf From Serving BS/ABS to Target BS/ABS

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	O	SFID associated with the Service Flow. This TLV SHALL be included if SF Info is included in the transmitted message.

IE	Reference	M/O	Notes
>>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).
>>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
>>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/ABS, to the Target BS/ABS.
>>>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	O	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 and also if an ARQ Discard was outstanding at the Serving BS/ABS before HO indication from MS/AMS is received.
>>>Reset Status	5.3.2.452	O	Indicates whether ARQ reset was pending at the Serving BS/ABS before HO. This TLV SHALL be included if ARQ Window Info is included in the transmitted message and also if an ARQ Reset was outstanding at the Serving BS/ABS before HO indication from MS/AMS is received.

4.7.8.5 Negotiating Data Integrity Method

HO related Data Integrity Methods are negotiated per service flow during the HO Preparation Phase. The entities involved in the Handover and Data Path Pre-Registration transactions negotiate the data integrity options among them.

The Data Integrity Capability TLV should be passed from the Serving BS, Target BS, and Anchor ASN-GW using Handover and Data Path Pre-Registration transactions.

During handover procedures, the Serving BS/ABS passes the Data Integrity Method TLVs indicating the data integrity options it supports to the Target BS/ABS via the HO Request message. The Data Integrity Applied TLV is also included in this message to indicate whether the DI method should be applied to a specific service flow or not. DI method is not supported for a service flow by default. If the Serving BS/ABS includes the Data Integrity Method TLV indicating data integrity options it supports in the HO Request message, the Target BS/ABS should respond by sending the Data Integrity Method TLVs indicating the data integrity options that both the Target and the Serving BS/ABS support to the Anchor ASN-GW in the Data Path Pre-Registration Request message. The Anchor ASN-GW SHALL determine which Data Integrity Method (s) should be used based on the Serving and Target BS/ABS data integrity options supported, its local policy, and Service Flow QoS information. if the BS/ABS Buffer Switching method supported and selected by both the Serving and Target BS/ABS, and supported by the Anchor ASN-GW, it SHALL be prioritized and selected by the Anchor ASN-GWas the data integrity option. The data integrity option selected by the Anchor ASN-GW for each service flow SHALL be passed to Target BS/ABSs using Data Path Pre-Registration Response messages. The Target BS/ABS then passes the final selection of Data Integrity Method TLV to the Serving BS/ABS via the HO Response message.

When the data integrity option is supported, the anchor ASN-GW SHALL apply the same data integrity method to all services flows to which data integrity is applied, for an MS session.

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 4-115 shows placing of the Data Integrity Method TLV in the structure of Path Pre-Registration Request/Response and HO Request/Response message.

Table 4-115 – Data Integrity Method TLV in 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	O	SFID associated with the Service Flow. This TLV SHALL be included if SF Info is included in the transmitted message.
>>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 (*HO Req*).
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	
>>Data Integrity Method	5.3.2.379	O	Serving-BS/ABS's Data Integrity Capability (*HO Req*).

Table 4-116 – Data Integrity Method TLV in Path_Pre-Reg_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	O	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 method selected by the Target BS/ABS.
>>>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/ABS.
BS Info	5.3.2.26	M	
>BS ID	5.3.2.25	M	
>>Data Integrity Method	5.3.2.379	O	Indicates mutual Data Integrity Method of Serving BS/ABS and Target BS/ABS.

Table 4-117 – 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	O	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	Indicate the authorized Data Integrity Method bitmask.
>>Data Path Info	5.3.2.45	O	

IE	Reference	M/O	Notes
>>>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/ABS.

4.7.9 ASN-anchored mobility with R6-Flex

This section discusses the intra-ASN handover procedures with R6-flex.

The high level procedure is as following. The Serving BS/ABS provides the address of the Anchor ASN-GW to the Target BS/ABS during MS/AMS handover. If the Target BS/ABS is in the same ASN as the Serving BS/ABS, the Target BS/ABS SHOULD establish R6 connectivity for this MS/AMS with the provided Anchor ASN-GW. With R6-flex it is still a valid option for the Target BS/ABS to establish a data path to the Anchor ASN-GW via the Serving GW acting as DPF relay (R4 data path).

Handover procedures using R6 interface between a BS and an Authenticator/ Anchor GW are presented in the section 4.7.2 and 4.7.3.

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/AMS and network. IPv6 support is optional for the MS/AMS 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 [94]. PMIP4 and PMIP6 (when IPv4 mode is enabled) require DHCPv4 support at the MS/AMS 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/AMS SHALL support either the DHCP or CMIP4 procedures described in this section for IP address acquisition. The network and MS/AMS SHALL support the DHCP procedures described in [25] for bootstrapping configuration information to the MS/AMS after IP address acquisition. Furthermore, the AMS and the network may implement and use FIAA for host configuration.

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 ([72]), or with Proxy Mobile IPv6 (PMIP6) [82]. An IPv6 MS/AMS MAY rely on address autoconfiguration,DHCPv6, or FIAA for its IPv6 address acquisition. The access network that provides IPv6 service SHALL support IPv6 configuration through stateless address autoconfiguration, one of the DHCP6 options, either Proxy or Relay mode, regardless of the mobility service assigned to the MS/AMS, and FIAA. Simultaneous PMIP6 and CMIP6 operation is not supported for the same MS/AMS. If an MS/AMS 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/AMS 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 MS/AMSs. 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/AMS is also assigned to the ASN GW to which this MS/AMS is attached. Some ASN entities, like DHCP Proxy, are originating IP datagrams destined to MS/AMSs. If the ASN entity originating a datagram destined for the MS/AMS and the MS/AMS is assigned the same private IP address as the MS/AMS, 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/AMS 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/AMS (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/AMS.

4.8.2 Proxy MIP4 R3 Mobility Management

The proxy Mobile IPv4 procedure is entirely done in the network and the MS/AMS is agnostic to the related procedures. There are certain events that take place with the MS/AMS e.g., MS/AMS requesting an IP address assignment at the connection setup time or the MS/AMS performing an handover across BS/ABS 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 4-136 (DHCP Proxy) and Figure 4-138 (DHCP Relay) and Figure 4-140 (FIAA).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/AMS Requirements

Requirements for DHCP support

The MS/AMS SHALL support the DHCP client function as defined in [25]. In order to acquire an IPv4 address, the MS/AMS SHALL send a DHCPDISCOVER message to the network over the initial service flow. Upon receiving the DHCPOFFER message from the network, the MS/AMS SHALL follow the procedures defined in [25] to select and configure an IPv4 address included in the DHCPOFFER message.

The MS/AMS 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 [26].

Requirements for FIAA support

The AMS MAY support the FIAA procedure. In order to acquire an IPv4 address using FIAA, the AMS SHALL send Host-Configuration-Capability-Indicator set to 1 and optionally the Requested-Host-Configurations IEs in the AAI-REG-REQ. Upon receiving the AAI-REG-RSP message including IPv4-Host-Address and possibly Additional-Host-Configurations IEs from the network, the MS SHALL configure its IPv4 address and other host parameters accordingly.

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/AMS.

4.8.2.1.2.1 DHCP Proxy Requirements

Upon receiving a DHCPDISCOVER message from the MS/AMS, 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/AMS 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/AMS.

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/AMS 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/AMS 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/AMS and respond back to the MS/AMS 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 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/AMS 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/AMS) as follows as default setting:

- T_1 = 0.5 * Lease Time
- T_2 = 0.875 * 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/AMS'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/AMS. This will make it looks like the MS/AMS 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 [26], [45] and [61] and [70].

The DHCP relay SHALL handle all DHCP messages sent by the MS/AMS to the broadcast IP address.

The DHCP relay is configured with the DHCP server address during the MS/AMS 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/AMS to the DHCP server.

Upon receiving a DHCPDISCOVER message from the MS/AMS, the DHCP relay SHOULD verify the “chaddr” field in the DHCP header matches the MS/AMS 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/AMS.

In case, the DHCP relay determines that the MS/AMS 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/AMS 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/AMS. 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/AMS. 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/AMS.

The DHCP relay behavior for handling DHCPREQUEST or DHCPDECLINE from the MS/AMS is same as in the case of DHCPDISCOVER.

When DHCP relay receives the DHCPREQUEST message from the MS/AMS, 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/AMS. 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/AMS. When DHCP relay receives the DHCPACK message from the DHCP Server, it SHALL relay the DHCPACK message to the MS/AMS.

Since AAA can assign different HAs (e.g., when dynamically assigning HA from a pool) and each HA handles different MS/AMS subnets, the assigned HA needs to be passed to DHCP server to allow choosing the matching MS/AMS address pool. DHCPDISCOVER and DHCPREQUEST from MS/AMS 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
result
Length:1
Value: MIPv4 registration result code as defined in RFC3344

Subopt-code (WiMAX DHCP relay agent subopt code): 2 – HA IP address
Length: Variable(either 4 or 16)
Value: IP address of HA
```

The DHCP relay SHALL intercept the DHCP renewal and release messages, verifying the content of the message. If R3 is not secured (e.g., by IPSec), the DHCP relay SHALL add the relay agent authentication suboption to the message before relaying it to the DHCP server.

For Dynamic HA assignment when both visited and home DHCP server addresses are available, DHCP relay SHALL select which DHCP server to be used, based on the local policy.

4.8.2.1.2.3 DHCP Server Requirements

The DHCP server SHALL support the procedures defined in [26], [45]and [61] and [70].

The DHCP server SHALL be located in the CSN. The DHCP server and the HA SHALL be located in the same CSN.

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 [70], 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 DHCP server needs to obtain a DHCP-RK to validate the authentication suboption messages, the server sends a AAA Access-Request packet to the local AAA server or in the Case of Diameter, the DHCP server SHALL support the WiMAX DHCP Diameter Application and send a WDHCPR command to the HAAA.

In the case of RADIUS, the DHCP server SHALL include the Message Authenticator (80) attribute used to integrity protect the Access-Request packet. The value of the Message-Authenticator attribute is set in accordance with the computation specified in [41].

When sending the RADIUS Access-Request packet or the WDHCPR command to the AAA server, the DHCP server SHALL include the following attributes:

- The RADIUS NAS-Identifier attribute or the Diameter Origin-Realm AVP set to the FQDN of the DHCP server originating the request.
- The NAS-IP-Address attribute or the Diameter Origin-Host AVP set to the IPv4 or IPV6 address of the DHCP server.
- The DHCPMSG-Server-IPv4 set to the address contained in the DHCPDISCOVER message if the DHCP server address in the DHCPDISCOVER message is different from the address contained in the DHCPv4-Serverattribute.
- The DHCP-RK-Key-ID set to the value of the Key-ID received as part of the authentication suboption in the DHCPDISCOVER message.

If the DHCP message received by the DHCP server includes the vendor specific relay agent suboption as defined in section 4.8.2.1.2.2 containing the MIP registration result, the DHCP server SHALL check it and include the appropriate reason in its response if the MIP registration has failed. The DHCP server SHALL process the DHCPDISCOVER and DHCPREQUEST messages sent by the relay agent and the DHCP Client according to [26]and [61].

All messages originated by the DHCP server SHALL always include the server identifier option set to its own IP address.

In the case when DHCP lease time expires, the DHCP server MAY inform the HA that the HoA assigned to an MS/AMS has expired. In response, the HA MAY send Registration Revocation to the FA, so that the PMIP4 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 FIAA Requirements

FIAA compliant ASN-GW and ABS MAY support FIAA.

4.8.2.1.3.1 ABS Requirements

ABS SHALL forward the FIAA-related IEs between the AAI-REG-REQ/RSP and MS_Attachment_Req/Rsp messages. These IEs include Host-Configuration-Capability-Indicator, Requested-Host-Configurations, IPv4-Host-Address, IPv6-Home-Network-Prefix, and Additional-Host-Configurations.

4.8.2.1.3.2 Advanced ASN-GW Requirements

The FIAA compliant ASN-GW prompts the collocated PMIP4 client to initiate the PMIP4 procedures when it receives Host-Configuration-Capability-Indicator set to 1 with the MS_Attachment-Req, If there had been no previously received HoA during the authentication phase, or no “Requested IP Address” option is used with Requested-Host-Configurations IE then the PMIP procedure will acquire a HoA from the home agent. Otherwise, the HoA obtained during authentication or IEEE 802.16m registration (AAI-REG-REQ/RSP) is sent in the PMIP registration request.

Upon receiving a response from the PMIP4 Client with an indication of successful PMIP4 registration, the Advanced ASN-GW SHALL extract the HoA that is assigned to the AMS and respond back to the AMS with a MS_Attachment_Rsp setting the IPv4-Host-Address IE to the received HoA. It MAY set the Domain Name Server option in the Additional-Host-configurations IE to the address of the DNS server when received in the RADIUS Access-Accept packet or Diameter WDEA command from the AAA server.

4.8.2.1.4 PMIP4 Client Requirements

Upon receiving an internal trigger from a DHCP proxy/relay or FIAA 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/relay or FIAA 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[20];
- 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 [49]. 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/AMS 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 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 or FIAA function with an indication of MIP4 registration success including the assigned HoA address(assigned HoA). Otherwise, the PMIP4 Client SHALL notify the DHCP proxy or FIAA function indicating the failed operation to acquire an IPv4 (HoA) for the Outer-Identity.

4.8.2.1.5 FA Requirements

FA SHALL operate as defined in [49] and [51].

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 [93] 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 [51] 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.

[20] 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.

4.8.2.1.6 HA Requirements

The HA SHALL process Mobile IPv4 messages as per [49] and [51]. 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 [49]. 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. If the MS/AMS BCE exists for the MS/AMS then the HA SHALL perform a AAA transaction only if the MN-HA SPI changes in order to fetch a new MN-HA key from the AAA server.

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 or FIAA 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 [49].

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*.

4.8.2.1.6.1 HA Requirements - Initial AAA-Request

Upon receiving RRQ for a MS/AMS for which there is no mobility binding exists, the HA SHALL send a RADIUS Access-Request or Diameter WHA4R command as per [38] 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. If the mobility binding exists for the MS/AMS, the HA SHALL send a AAA Access-Request if the MN-HA SPI is different from the SPI received in previously received RRQ message. This is done in order to fetch a new MN-HA key, which may have changed after re-authentication.

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 [41] 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.

4.8.2.1.6.2 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 [41]. 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 [75].

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 WACR command (Start) message for that the Mobile IPv4 session.

4.8.2.1.6.3 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.

4.8.2.1.6.4 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 WACA 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).

4.8.2.1.7 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 [69] 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 [41]. 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/AMS 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/AMS 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 [41].

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 [63], during the DHCP authentication sub-option procedure, when the DHCP sever 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 [41]. 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 [41].

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.

4.8.2.1.8 PMIP4 Connection Setup Call Flow

The following sections describe the PMIP4 Connection Setup procedure using DHCP (proxy and relay mode) and FIAA.

4.8.2.1.8.1 DHCP Proxy in ASN

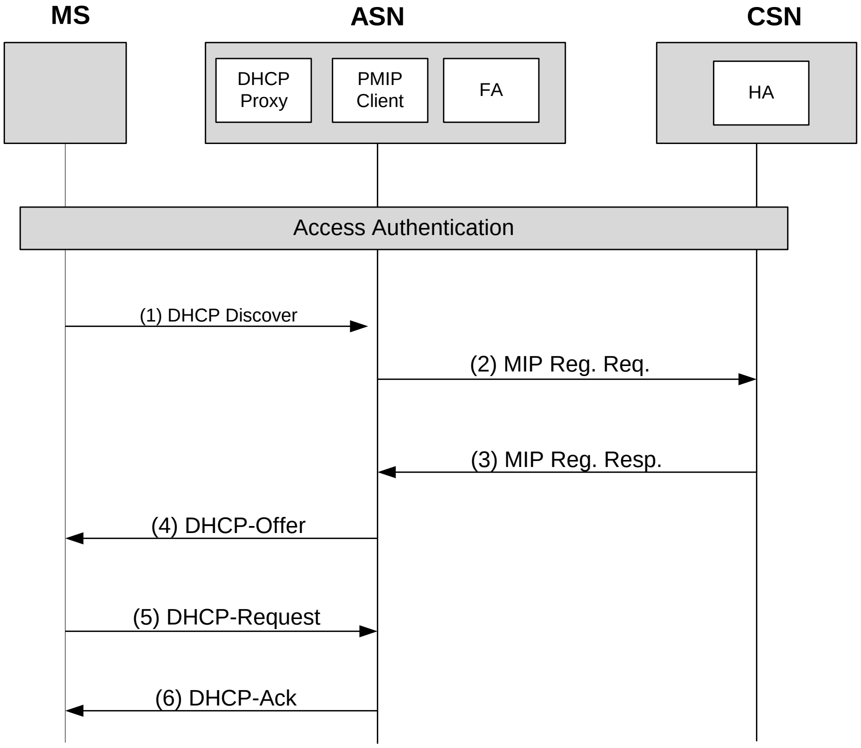


Figure 4-136– PMIP4 Connection Setup Procedure

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/AMS 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/AMS. A minimal number of DHCPOFFER messages should be sent, preferably only one.

STEP 5

MS/AMS 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 [25] by sending the DHCPACK message.

4.8.2.1.8.2 DHCP Proxy in ASN - DHCP Request message specifies the MS/AMS previously assigned IP address

In this scenario, after performing successful network entry EAP authentication, the DHCP client in MS/AMS is trying to obtain the same IP address e.g., the DHCP lease timer from a previous network entry has not expired. The MS/AMS, in this case, uses the DHCP Request message to indicate the requested IP address.

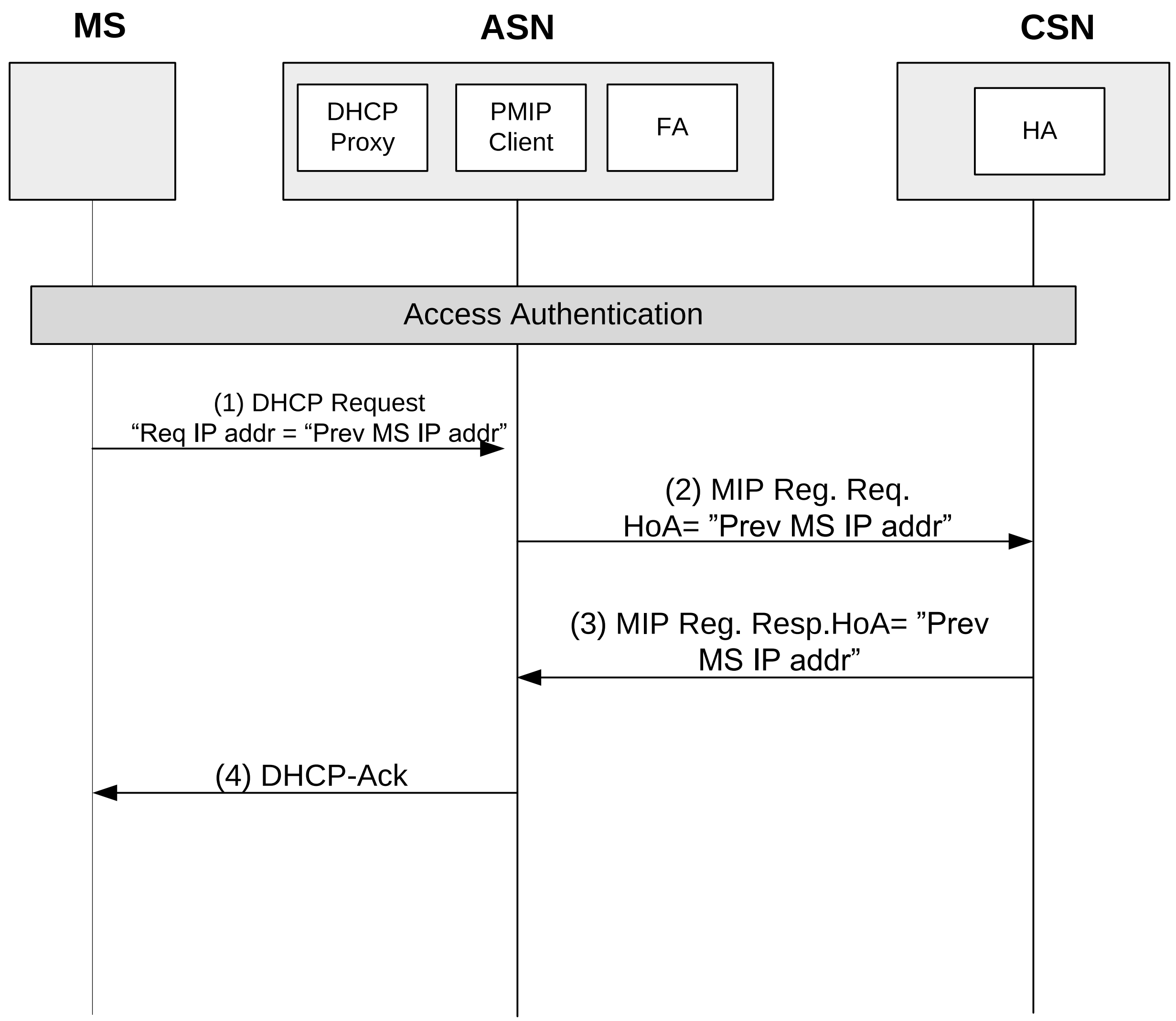


Figure 4-137– DHCP Session Renewal in PMIP4 case via DHCP Request - DHCP Proxy in ASN

STEP 1

The MS/AMS 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/AMS, DHCP Proxy SHALL send DHCPNAK to the MS/AMS, the DHCP Client will behave as specified in [25]. And MIP Registration procedure (STEP 2 - 4) SHALL be skipped.

STEP 2 - 3

Upon receiving the DHCP REQUEST from the MS/AMS, 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/AMS, 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/AMS or can't assign the requested HoA to the MS/AMS, 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/AMS and skips step 4.

STEP 4

The Anchor ASN SHALL process the DHCP Request message and reply with a DHCP Ack to MS/AMS.

In case of the MIP failure, the DHCP Proxy/PMIP Client SHALL send DHCPNAK message to MS/AMS. Then the DHCP Client will behave as specified in [25].

4.8.2.1.8.2.1 DHCP Proxy in ASN Timers and Timer Considerations

All timers are set and cleared according to DHCP ([25]) and MIP ([49]) specifications.

4.8.2.1.8.3 DHCP Relay in ASN

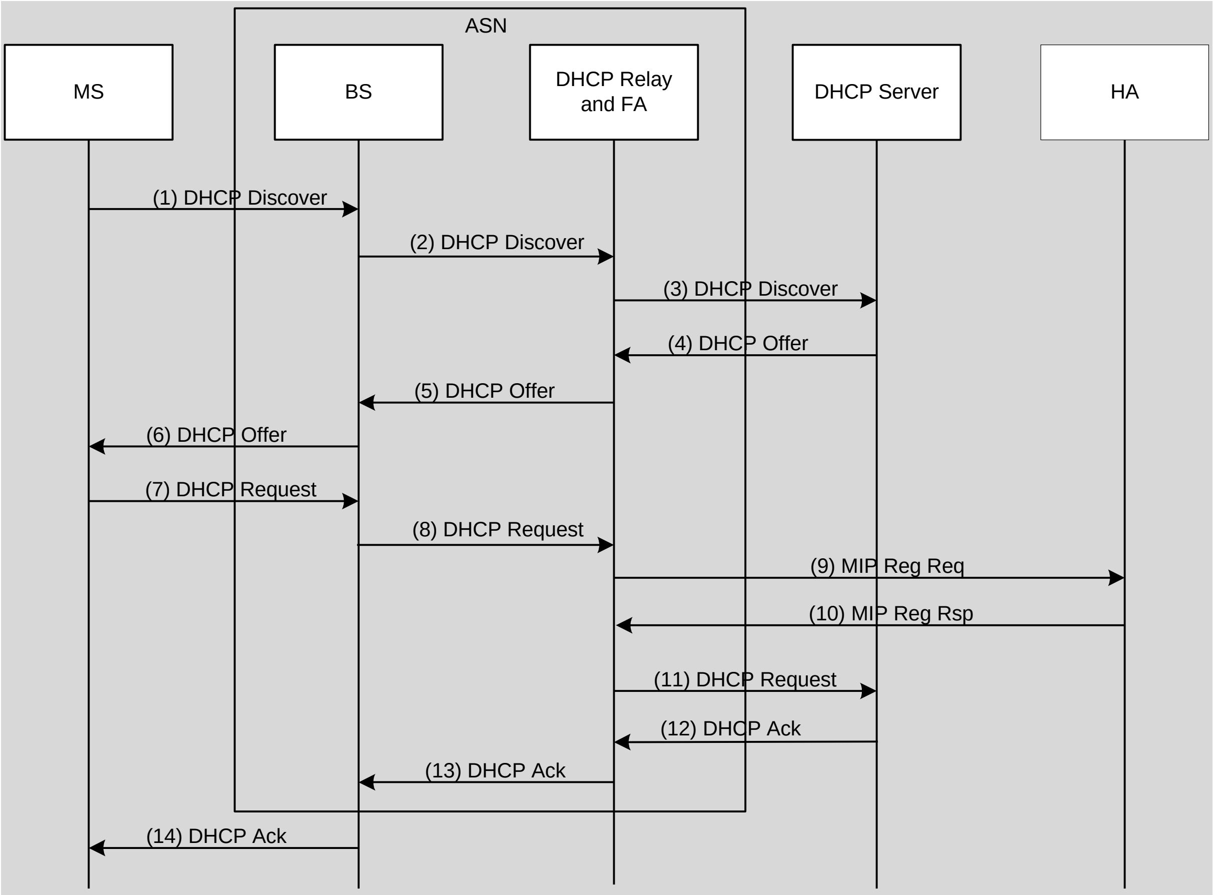


Figure 4-138– PMIP4 Connection Setup - DHCP Relay in ASN

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 [66] to have data integrity and replay protection for relayed DHCP messages.

STEP 1

The MS/AMS sends a DHCP Discover as a broadcast message. The DHCP message is sent on the MS/AMS's Initial service flow setup over R1 interface to the BS/ABS.

STEP 2

The DHCP Discover message is forwarded from BS/ABS 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/AMS 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/AMS or per SF, the MS/AMS context can be found based on the Datapath and not on the MAC address. If the Datapath is per BS/ABS the MS/AMS context can be found based on the MAC address or MS/AMS 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/AMS. The DHCP Offer message is sent from ASN GW to BS/ABS through the Data Path.

The destination IP address of the DHCP Offer message sent to MS/AMS is a unicast one. Normally DHCP servers or relay agents attempt to deliver the DHCP Offer to a MS/AMS directly using unicast delivery. Unfortunately some MS/AMS's implementations are unable to receive such unicast IP datagram until they know their own IP addresses. To work around with this kind of MS/AMSs, 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/AMS.

STEP 6

BS/ABS sends DHCP Offer message to the MS/AMS on the MS/AMS's Initial Service Flow.

STEP 7

MS/AMS 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/ABS 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/AMS. 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/AMS.

STEP 13

The DHCP Relay relays the DHCP Ack to the BS/ABS.

STEP 14

BS/ABS sends DHCP Ack message to the MS/AMS on the MS/AMS's provisioned Initial Service Flow.

If MS/AMS 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/AMS SHALL restart the IP initialization process.

4.8.2.1.8.3.1 DHCP Relay in ASN Error Conditions

4.8.2.1.8.3.1.1 Timers and Timer Considerations

All timers are set and cleared according to DHCP ([25]) and MIP ([49]) specifications.

4.8.2.1.8.3.1.2 Proxy MIP Registration Error Considerations

The DHCP Server confirms the PoA address allocation to this MS/AMS 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/AMS.

4.8.2.1.8.3.1.3 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.

4.8.2.1.8.4 DHCP Relay in ASN - DHCP Request message specifies the MS/AMS previously assigned IP address

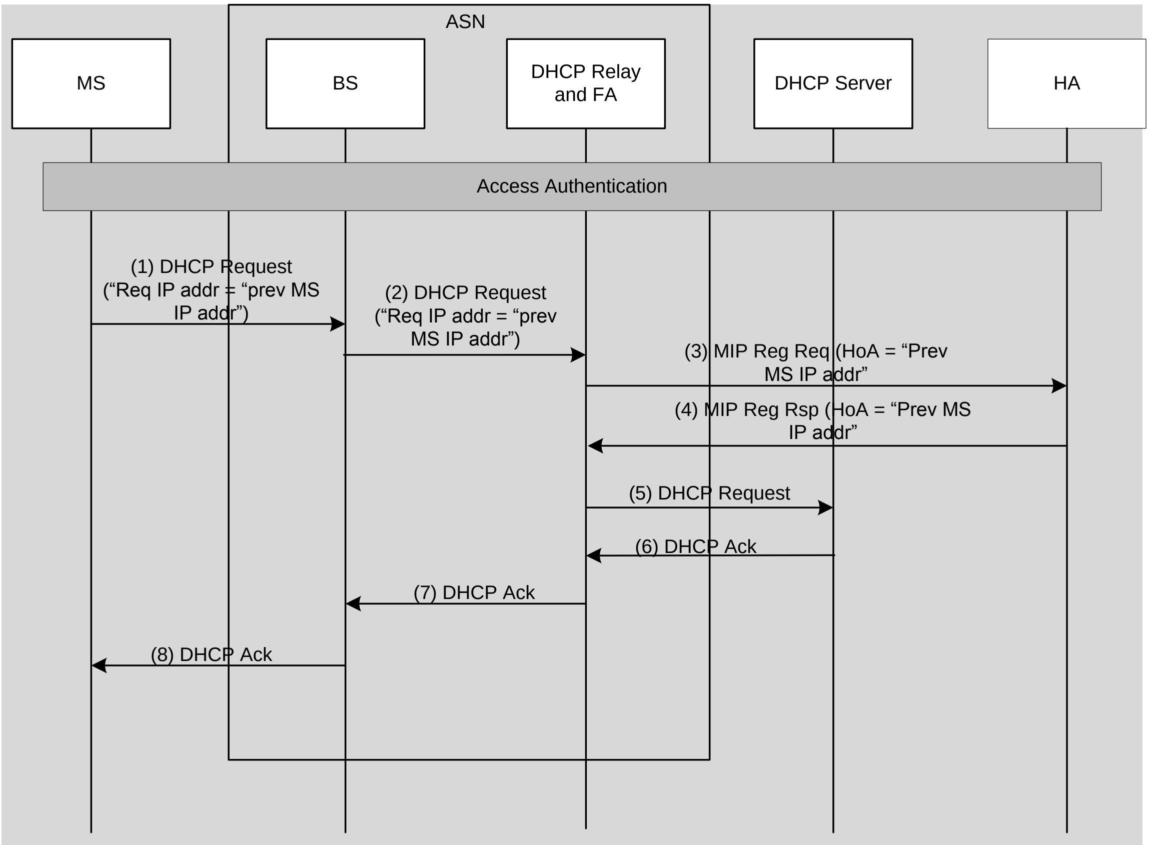

ASN
MS
BS
DHCP Relay and FA
DHCP Server
HA
Access Authentication
(1) DHCP Request (“Req IP addr = “prev MS IP addr”)
(2) DHCP Request (“Req IP addr = “prev MS IP addr”)
(3) MIP Reg Req (HoA = “Prev MS IP addr”
(4) MIP Reg Rsp (HoA = “Prev MS IP addr”
(5) DHCP Request
(6) DHCP Ack
(7) DHCP Ack
(8) DHCP Ack

Figure 4-139 - 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/AMS is trying to obtain the same IP address because the DHCP lease timer from a previous network entry has not expired. The MS/AMS, in this case, uses the DHCP Request message to indicate the requested IP address

STEP 1

The MS/AMS sends a DHCP Request to the BS/ABS in order to renew its IP address, Required IP address field is set to MS/AMS previous IP address.

STEP 2

DHCP Request message is sent from BS/ABS to DHCP relay in ASN through the Data Path established.

STEP 3

Upon receiving the DHCP REQUEST from the MS/AMS, the DHCP Relay/PMIP Client sends the MIP RRQ message to the HA with home address filed 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/AMS 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/AMS, the HA SHALL reject the MIP Registration Request by sending MIP Registration Reply with Code set to 129- ‘administratively prohibited’.

The HA IP address policy and assignment is outside the scope of this specification.

STEP 5

After the establishment of MIP tunnel the PMIP client informs the DHCP Relay with 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.

The DHCP relay MAY send a unicast DHCP Request message to each DHCP server listed in the Access-Accept message.

If DHCP Server receives MIP rejection in vendor specific relay agent suboption, the DHCP Server consequently sends DHCP NAK to the MS/AMS.

STEP 6

The DHCP server receives the DHCP Request and replies with a DHCP Ack containing the configuration information requested by the MS/AMS.

STEP 7

The DHCP Relay relays the DHCP Ack to the BS/ABS.

STEP 8

BS/ABS sends DHCP Ack message to the MS/AMS on the MS/AMS’s provisioned Initial Service Flow.

If MS/AMS doesn’t receive a DHCP Ack, or DHCP Nak message when timeout, it will retransmit DHCP Request as specified in [25]. If neither DHCP Ack nor DHCP Nak received when the maximum retransmission reached, the DHCP Client in MS/AMS will behave as specified in [25].

4.8.2.1.9 FIAA-based Connection Setup

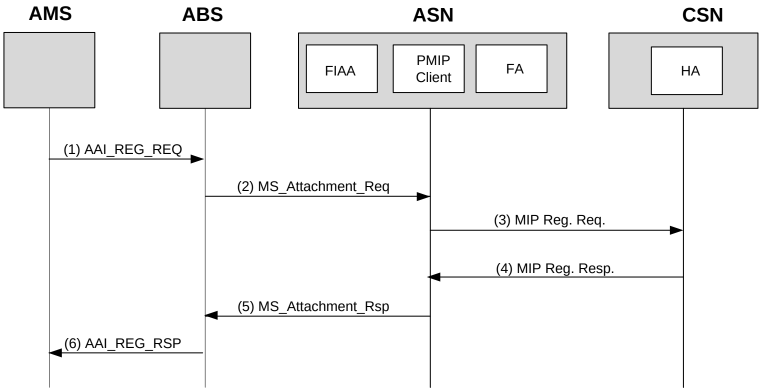


Figure 4-140 - PMIP4 Connection Setup procedure using FIAA

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.

AMS sends AAI-REG-REQ message as part of its network entry procedure. If the AMS wants to request a known IP address using FIAA, it includes Requested-Host-Configurations IE that carries Requested-IP-Address option carrying that IP address value in addition to Host-Configuration-Capability-Indicator IE set to 1. Otherwise the AMS includes Host-Configuration-Capability-Indicator IE set to 1 (i.e., Requested-Host-Configurations IE is not used).

Step 2.

ABS generates MS_Attachment_Req and copy the FIAA IEs to that message.

Step 3.

Upon receiving the FIAA IEs, the FIAA function triggers the PMIP4 client to initiate the Mobile IPv4 Registration procedure. If HoA was received during access authentication or the IEEE 802.16m registration procedure, then the PMIP4 client uses the HoA information and constructs a Mobile IPv4 Registration Request message. Otherwise, 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 4.

If an HoA is 0.0.0.0 in the Mobile IP Registration Request message, the HA assigns an HoA. Otherwise, the HoA requested in the Mobile IP Registration Request message is assigned. 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 5.

The PMIP4 client passes this information to the FIAA function which generates the FIAA IEs to be sent along with the MS_Attachment_Rsp. The FIAA compliant ASN-GW sends the MS_Attachment_Rsp to the ABS.

Step 6.

ABS delivers the FIAA IEs to the AMS via AAI-REG-RSP message. AMS processes these IEs and configures its IP address and other parameters accordingly.

All timers are set and cleared according to IEEE 802.16m [105] and MIP [49] specifications.

4.8.2.2 Proxy MIP4 Session Renewal Procedure

The PMIP4 Client SHALL refresh the MIP4 binding with the FA and the HA on behalf of the MS/AMS. This procedure is transparent to the MS/AMS since the DHCP RENEW and REBIND states (when DHCP is used) and IEEE 802.16m registration state (when FIAA is used) are not tied to the Mobile IPv4 Registration Lifetime (which the MS/AMS is unaware of). Figure 4-141 – PMIP4 Session Renewal Procedure

shows steps involved in Proxy MIP4 Session Renewal procedure.

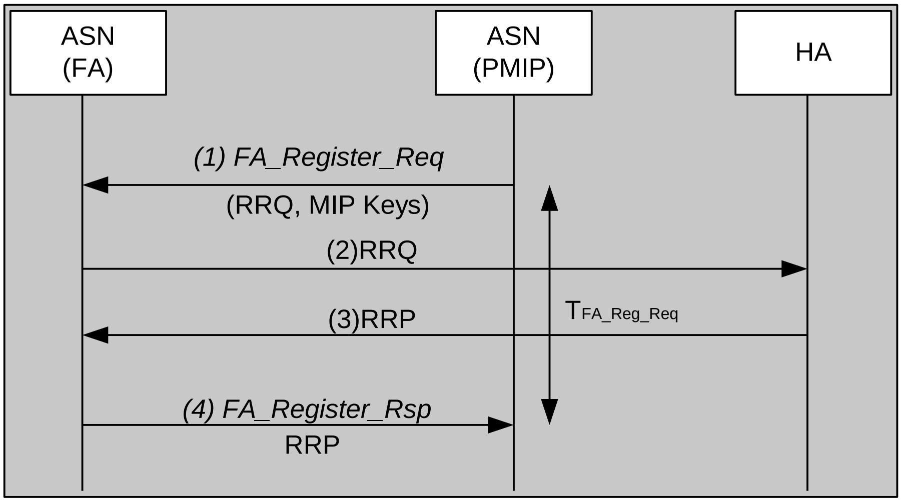


Figure 4-141 – PMIP4 Session Renewal Procedure

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/AMS 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 $T_{FA\_Reg\_Req}$[21] 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/AMS Requirements

When DHCP is used, the MS/AMS SHALL support the DHCP client function as defined in [26] for the IP address renewal procedure. The address renewal by the MS/AMS SHALL be based on the T1 (RENEW) and T2 (REBIND) timers as defined in the RFC.

When FIAA is used, the allocated IP address is persistent throughout the WiMAX session. It does not have to be renewed.

[21] The value of $T_{FA\_Reg\_Req}$ and retransmission behavior should be per RFC3344.

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 [26]. When the DHCP proxy receives a DHCPREQUEST message from the MS/AMS for an IPv4 address for which the Lease Time is either close to T1 or T2 value, it SHALL respond back to the MS/AMS 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/AMS will be terminated by the DHCP proxy collocated with anchor DPF/FA.

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/AMS. The DHCP relay SHALL perform the verification of the ‘chaddr’ field in the DHCP message and other security related checks as described in 4.8.2.1.8.3.1. DHCP relay SHALL relay the DHCP message to the DHCP server in the CSN, in accordance with the [45]. If R3 is not secured (e.g., by IPsec), the DHCP relay SHALL authenticate relayed DHCP messages by providing the relay agent authentication suboption ([66]).

4.8.2.2.3 FIAA Requirements

When FIAA is used, the allocated IP address is persistent throughout the WiMAX session. It does not have to be renewed. Therefore there are no requirements and procedures for renewing IP addresses with FIAA.

4.8.2.2.4 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 4.8.2.3.8.1.

4.8.2.2.5 FA Requirements

The FA requirements are the same as section 4.8.2.1.5.

4.8.2.2.6 HA Requirements

The HA SHALL process the RRQ for binding renewal for an existing binding cache entry the same way as defined in section 4.8.2.1.6.

4.8.2.2.7 AAA Server Requirements

Same as section 4.8.2.1.7.

4.8.2.2.8 PMIP4 Session Renewal Call Flows

4.8.2.2.8.1 DHCP Session Renewal Flows

4.8.2.2.8.1.1 DHCP Proxy

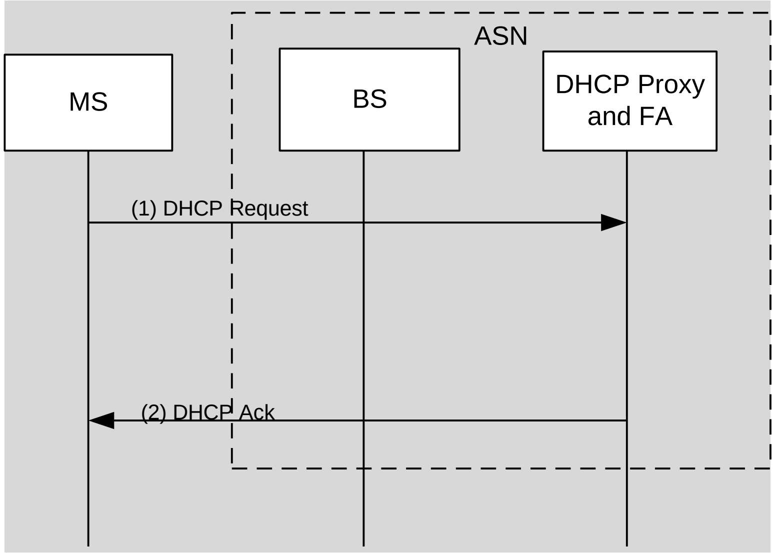


Figure 4-142 – DHCP Session Renewal in PMIP4 case- DHCP Proxy in ASN

STEP 1

The MS/AMS 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/AMS.

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/AMS MAY initiate network exit. If the MS/AMS does not receive any response from the DHCP Proxy, the MS/AMS does number of retries and then MAY initiate network exit.

4.8.2.2.8.1.2 DHCP Relay in ASN

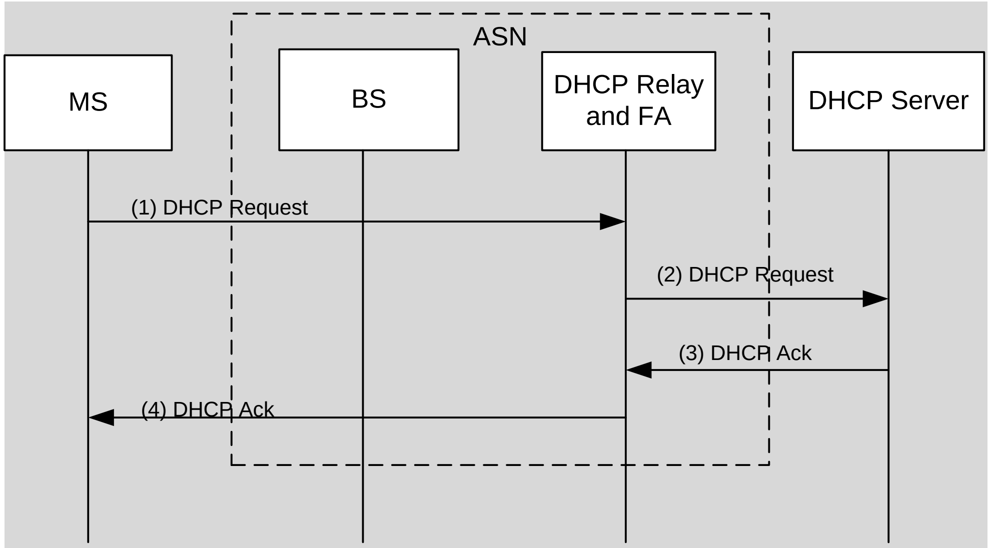


Figure 4-143 – DHCP Session Renewal in PMIP4 case- DHCP Relay in ASN

STEP 1

The MS/AMS 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/AMS. 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/AMS may initiate Network exit. If the MS/AMS does not receive any response from the DHCP server the MS/AMS does number of retries and then MAY initiate Network exit.

4.8.2.2.8.1.2.1 DHCP Relay in ASN Timers and Timer Considerations

All timers are set and cleared according to DHCP ([25]) and MIP ([49]) specifications.

4.8.2.2.8.2 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 4.8.2.3.8. This section describes CSN anchored mobility handover without re-authentication.

If the FA relocation is due to MS/AMS 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 4.6.5. 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/AMS 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/AMS. 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 4-118 – 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 (one or two)	5.3.2.56	O	Information about the DHCP Relay. Anchor ASN SHALL include this TLV if operating in DHCP Relay mode. Two instances of this TLV are present for dual stack case.
>>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 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

IE	Reference	M/O	Notes
			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.
>>>IPv6 Flow Label	5.3.2.470	O	
>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 (one or two)	5.3.2.54	O	Anchor ASN SHALL include this TLV when operating in Proxy DHCP mode. Two instances of this TLV are present for dual stack case.
>>>IP Remained Time	5.3.2.83	O	Remaining lease time for the assigned IP address. This TLV SHALL be included if DCHP 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

IE	Reference	M/O	Notes
			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 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	CM	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/AMS session. If Target ASN does not support any of the required online accounting capabilities, it SHOULD reject Anchor DPF

IE	Reference	M/O	Notes
			relocation procedure.
>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 4-119 – 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/AMS 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	CM	This TLV SHALL be Present as a part of HLD Relocation; when HLD is Collocated in FA.

IE	Reference	M/O	Notes
>> 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	

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 (available only when DHCP is used) along with other Layer3 context maintained by the Anchor ASN for the MS/AMS SHALL be transferred to the target ASN. The PMIP4 Client SHALL initiate a MIP4 registration on behalf of the MS/AMS 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 4-120 – 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/ABS. 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/ABS must update its notion of the location of the anchor DPF function for this MS/AMS. The serving BS/ABS SHALL confirm the receipt of the Context_Rpt message by sending the Context_Ack message.

Table 4-121– Context_Rpt from Target FA to Serving BS/ABS

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Set to indicate “MS/AMS 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 4-122– Context_Ack from Serving BS/ABS 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/AMS Requirements

There are no specific MS/AMS 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/AMS, once it receives a success indication from the Target ASN that FA has been relocated.

4.8.2.3.2.2 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/AMS. In the course of the R3 relocation, the address of the DHCP server is transferred as part of the MS/AMS 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/AMS. 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 [45]. If R3 is not secured (e.g., by IPsec), the DHCP relay SHALL authenticate relayed DHCP messages by providing the relay agent authentication suboption ([66]).

4.8.2.3.3 FIAA Requirements

There are no specific requirements about FIAA for CSN anchored mobility management with PMIP4.

4.8.2.3.4 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/AMS 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 4-123 – 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	5.3.2.101	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 4-124 – 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	
>FA-HA SPI	5.3.2.68	O	

Table 4-125 – FA_Register_Rsp Message

IE	Reference	M/O	Notes
RRP	5.3.2.97	M	Defined in MIP RFC.

Table 4-126 – 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.

4.8.2.3.5 FA Requirements

In general the requirements specified in 4.8.2.1.5 SHALL apply to the FA.

4.8.2.3.6 HA Requirements

The HA SHALL process the RRQ the same way as defined in 4.8.2.1.6. The HA SHALL modify the binding cache entry for the MS/AMS 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/AMS to the new CoA. The HA MAY send Revocation message to the previous FA to terminate binding.

4.8.2.3.7 AAA Server Requirements

There are no specific AAA Server requirements for CSN anchored mobility management with PMIP4.

4.8.2.3.8 PMIP4 Mobility Procedure

4.8.2.3.8.1 PMIP4 CSN MM Handover

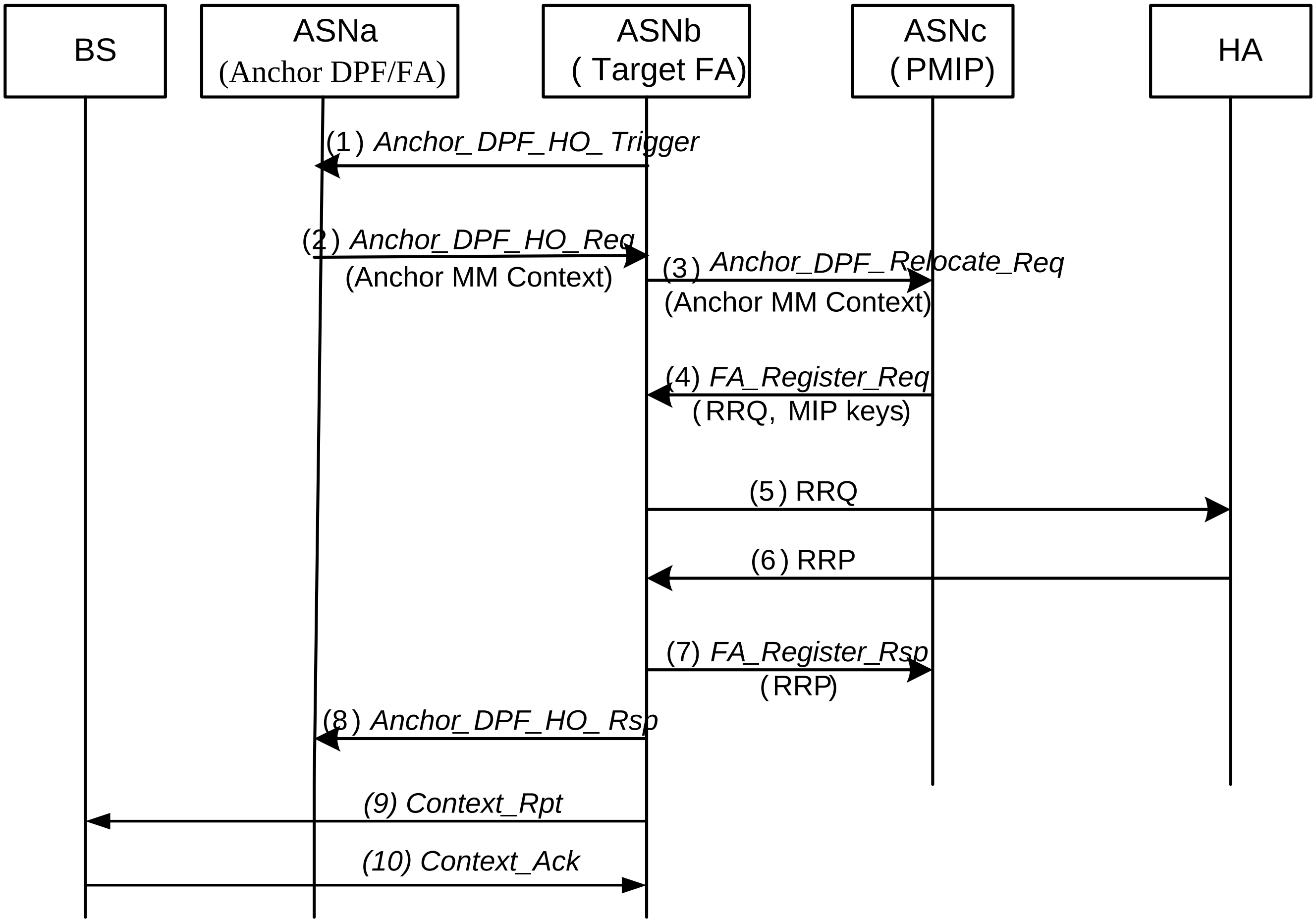


Figure 4-144 – CSN-Anchored Mobility (PMIP)

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. 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 DHCP context information for the MS/AMS and the Authenticator Id (Authenticator is co-located with the PMIP client) which is used to locate the PMIP client, and ASNa will start a timer $T_{Anchor\_DPF\_HO\_Req}$[22] for *Anchor_DPF_HO_Rsp* from ASNb.

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 $T_{Anchor\_DPF\_Relocate\_Req}$ 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 [49], 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/AMS 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 $T_{FA\_Reg\_Req}$[23] is started for *FA_Register_Rsp* from ASNb.

STEP 5

After receiving *FA_Register_Req*, ASNb stops $T_{Anchor\_DPF\_Relocate\_Req}$. The target FA relays the RRQ to the HA.

STEP 6

The HA responds with the RRP.

STEP 7

The target ASN relays the MIP RRP encapsulated in an *FA_Register_Rsp* message to the PMIP4 client. The PMIP4 client updates the FA in its record and stops $T_{FA\_Reg\_Req}$. 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 $T_{Anchor\_DPF\_HO\_Req}$ started in step 2. Either ASNa or ASNb initiate Path

[22] $T_{Anchor\_DPF\_HO\_Req}$ value should be larger than the sum of $T_{AnchorDPF\_Relocate\_Request}$ and $T_{FA\_Register\_Request}$ including retransmission

[23] The value of $T_{FA\_Reg\_Req}$ and retransmission behavior should be per [49].

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 $T_{Anchor\_DPF\_HO\_Req}$ started in step 2.

STEP 9

ASNb sends Context Report to the BS/ABS. The Context_Rpt message contains the address of the new anchor DPF function.

STEP 10

BS/ABS updates location of the anchor DPF function for this MS/AMS upon receipt of the Context_Rpt message. The BS/ABS confirms the receipt of the Context_Rpt message by sending the Context_Ack message.

4.8.2.3.8.1.1 PMIP4 CSNMM Handover Timers and Timer Considerations

This section provides the description of the timer used during PMIP4 CSN MM Handover.

- $T_{Anchor\_DPF\_HO\_Trigger}$: is started by target ASNb upon sending an *Anchor_DPF_HO_Trigger* message. It is stopped upon receiving a corresponding *Anchor_DPF_HO_Req*.
- $T_{Anchor\_DPF\_HO\_Req}$: is started when serving ASNa sends an *Anchor_DPF_HO_Req* and is stopped upon receiving a corresponding *Anchor_DPF_HO_Rsp*.
- $T_{Anchor\_DPF\_Relocate\_Req}$: is started by the target ASNb when the *Anchor_DPF_Relocate_Req* is sent on R4. It is stopped upon receiving a corresponding *FA_Register_Req*.
- $T_{FA\_Reg\_Req}$: is started by the PMIP4 client when the *FA_Register_Req* is sent on R4. It is stopped upon receiving a corresponding *FA_Register_Rsp*.

Table 4-127 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-127 – Timer Values for PMIP4 CSN MM Handover Messages over R4/R3

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{Anchor\_DPF\_HO\_Trigger}$	TBD		TBD
$T_{Anchor\_DPF\_HO\_Req}$	TBD		TBD
$T_{Anchor\_DPF\_Relocate\_Req}$	TBD		TBD
$T_{FA\_Reg\_Req}$	TBD		TBD

4.8.2.3.8.1.2 PMIP4 CSN MM Handover Error Conditions

This section describes error conditions associated with the PMIP4 CSN MM Handover procedure.

4.8.2.3.8.1.2.1 Timer Expiry

Table 4-128 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 4-128 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{Anchor\_DPF\_HO\_Trigger}$	Target FA	PMIP4 CSN MM handover is aborted and further action of Serving/Target FA is implementation Specific.
$T_{Anchor\_DPF\_HO\_Req}$	Serving FA	PMIP4 CSN MM handover is aborted and further action of Serving/Target FA is implementation Specific.
$T_{Anchor\_DPF\_Relocate\_Req}$	Target FA	PMIP4 CSN MM handover is aborted and *Anchor_DPF_HO_Rsp* is sent to ASNa with Result Code set to Failure.
$T_{FA\_Register\_Req}$	PMIP4 client	PMIP4 CSNMM Handover is aborted.

4.8.2.3.8.1.2.2 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.

4.8.2.3.8.1.2.3 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/AMS sending a DHCPRELEASE message (when DHCP is used);
- The IP address lease timer expires at the DHCP proxy/DHCP Relay (when DHCP is used) 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/AMS and send Registration Revocation message to the FA (Refer to [51]).

For PMIP4 session termination triggered network exit, see section 4.5.1.2.4.

4.8.2.4.1 MS/AMS Requirements

When the MS/AMS 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 when it uses DHCP.

4.8.2.4.2 DHCP Requirements

4.8.2.4.2.1 DHCP Proxy

Upon receiving a DHCPRELEASE from the MS/AMS 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/AMS.

The DHCP proxy SHALL release the IPv4 address lease (HoA) and any associated state for the MS/AMS 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/AMS, 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/AMS.

4.8.2.4.3 FIAA Requirements

There are no requirements on FIAA for PMIP4 Termination. There is no explicit FIAA message for terminating the IP address configuration. Network exit procedure constitutes termination in this case.

4.8.2.4.4 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 4-129 – 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 4-130 – FA_Revoke_Rsp

IE	Reference	M/O	Notes
Result Code	5.3.2.154	M	Result of Revoke, Success or failure indication.

4.8.2.4.5 FA Requirements

There is no specific requirement on the FA for the termination process.

4.8.2.4.6 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.

4.8.2.4.7 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.

4.8.2.4.8 PMIP4 Session Release Procedure

4.8.2.4.8.1 PMIP4 Session Release

4.8.2.4.8.1.1 MS/AMS Initiated PMIP4 Session Release when using DHCP

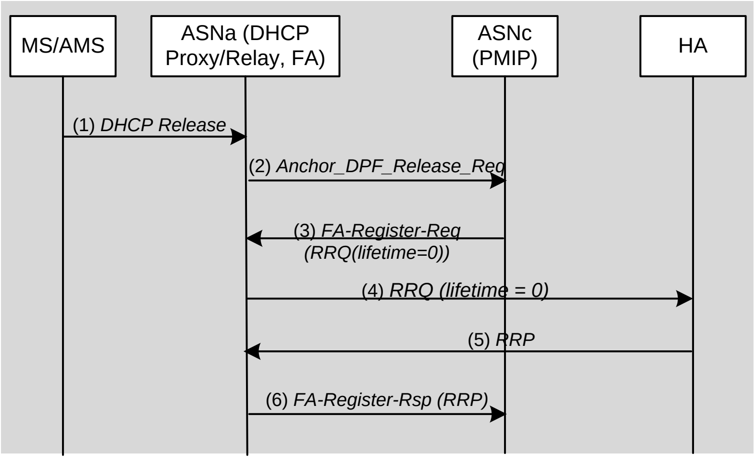


Figure 4-145 – PMIP4 Session Release Triggered by MS/AMS

STEP 1

The trigger can be initiated by MS/AMS 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 $_{\text{Anchor\_DPF\_Release\_Req}}$ 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 $_{\text{Anchor\_DPF\_Release\_Req}}$, 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/AMS, it is operator/network policy, when to trigger Network Exit for the MS/AMS as specified in section 4.5.2.

4.8.2.4.8.1.1.1 MS/AMS Initiated PMIP4 Session Release Timer and Timing Consideration

This section identifies the timer used during MS/AMS Initiated PMIP4 Session Release procedure.

- T $_{\text{Anchor\_DPF\_Release\_Req}}$: 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 4-131 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-131 – Timer Values for MS/AMS Initiated PMIP4 Session Release Messages over R4/R3

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
T $_{\text{Anchor\_DPF\_Release\_Req}}$	TBD		TBD

4.8.2.4.8.1.1.2 MS/AMS Initiated PMIP4 Session Release Error Conditions

This section describes error conditions associated with the MS/AMS Initiated PMIP4 Session Release procedure.

4.8.2.4.8.1.1.2.1 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 4-61.

Table 4-132 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
T $_{\text{Anchor\_DPF\_Release\_Req}}$	AnchorDPF ASN	Behave as if FA-Register-Req is received. The Context information remained on PMIP4 and HA is released based on their time-out mechanism, which is implementation dependent.

4.8.2.4.8.1.2 ASN Initiated PMIP4 Session Release

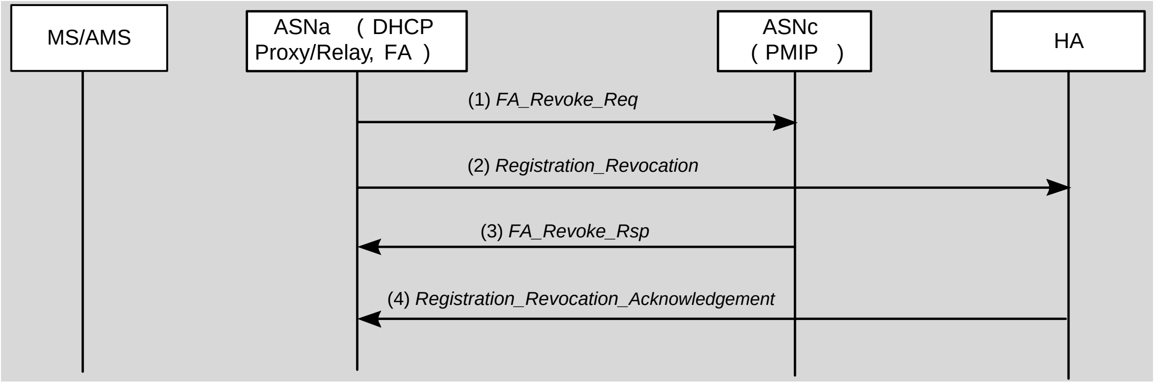

MS/AMS
ASNa (DHCP Proxy/Relay, FA)
ASNc (PMIP)
HA
(1) FA_Revoke_Req
(2) Registration_Revocation
(3) FA_Revoke_Rsp
(4) Registration_Revocation_Acknowledgement

Figure 4-146 – 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 4.8.2.4.8.1.1 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*[24].

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.

4.8.2.4.8.1.2.1 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 4-133 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-133 – 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

[24] The timer for Registration Revocation Message sent to the HA and retransmission behavior should be per [51].

4.8.2.4.8.1.2.2 ASN Initiated PMIP4 Session Release Error Conditions

This section describes error conditions associated with the ASN Initiated PMIP4 Session Release procedure.

4.8.2.4.8.1.2.2.1 Timer Expiry

Table 4-134 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 4-52.

Table 4-134 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{FA\_Revoke\_Req}$	AnchorDPF ASN	Behave as if both *FA_Revoke_Rsp* are received. The Context information remained on PMIP4 and HA is released based on their time-out mechanism, which is implementation dependent.

4.8.2.4.8.1.3 HA Initiated PMIP4 Session Release

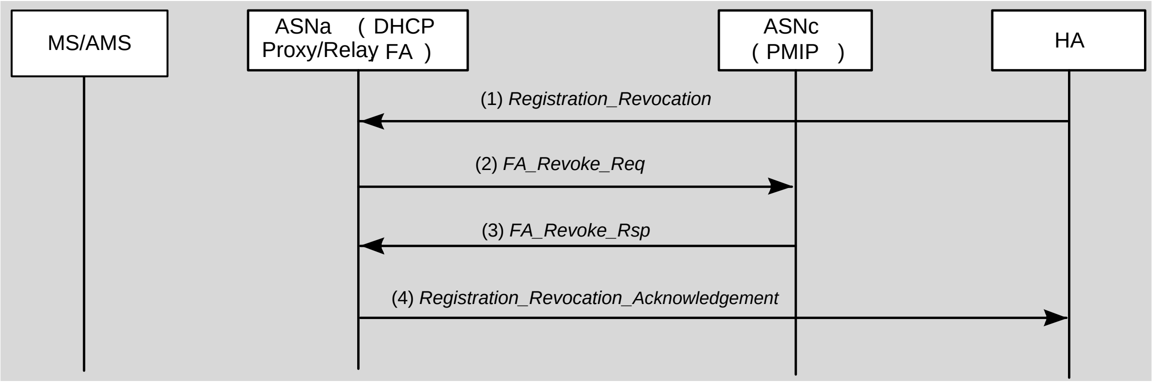

MS/AMS
ASNa (DHCP Proxy/Relay FA)
ASNc (PMIP)
HA
(1) Registration_Revocation
(2) FA_Revoke_Req
(3) FA_Revoke_Rsp
(4) Registration_Revocation_Acknowledgement

Figure 4-147 – 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 $T_{Registration\_Revocation}$ to wait for *Registration_Revocation_Acknowledgement*[25].

STEP 2

FA receiving *Registration_Revocation* sends *FA_Revoke_Req* to PMIP4 client and starts $T_{FA\_Revoke\_Req}$ timer.

STEP 3

PMIP4 client upon receiving *FA_Revoke_Req* sends *FA_Revoke_Rsp* to FA.

[25] The timer for Registration Revocation Message sent by the HA and retransmission behavior should be per [51].

STEP 4

FA receiving *FA_Revoke_Rsp* stops the timer $T_{FA\_Revoke\_Req}$, deletes the PMIP context of the MS/AMS and sends *Registration_ Revocation _Acknowledgement* to HA. HA on receiving *Registration_Revocation_Acknowledgement* message stops $T_{Registration\_Revocation}$ timer.

4.8.2.4.8.1.3.1 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 4-135 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-135 – Timer Values for HA Initiated PMIP4 Session Release Messages

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{Registration\_Revocation}$	TBD		TBD

4.8.2.4.8.1.3.2 HA Initiated PMIP4 Session Release Error Conditions

This section describes error conditions associated with the HA Initiated PMIP4 Session Release procedure.

4.8.2.4.8.1.3.2.1 Timer Expiry

Table 4-136 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 4-52.

Table 4-136 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{Registration\_Revocation}$	HA	Behave as if *Registration_Acknowledgement* is received and release the MIP tunnel.

4.8.2.4.8.1.4 R3 Session Release – Initiated by Authenticator or AAA

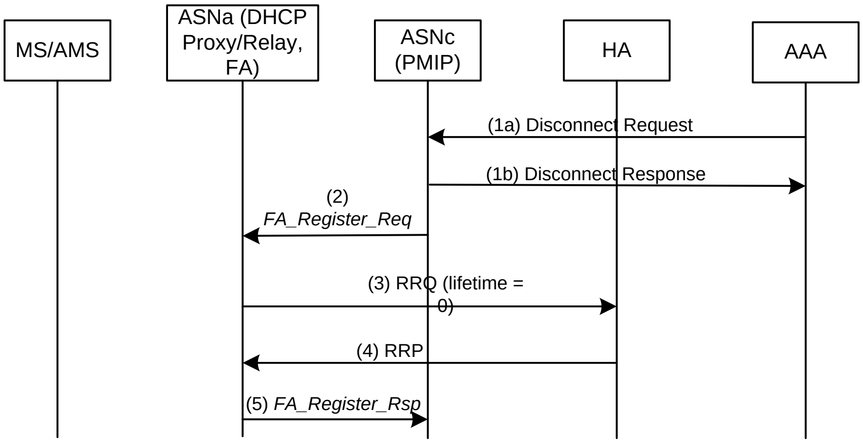


Figure 4-148 – PMIP4 Session Release triggered by Authenticator or AAA

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*.

4.8.2.4.8.1.4.1 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 4.8.2.3.8.1.1.

4.8.2.4.8.1.4.2 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.

4.8.2.4.8.1.4.2.1 Timer Expiry

Table 4-137 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 4-137.

Table 4-137 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{FA\_Register\_Req}$	PMIP4 client	Behaves as if PMIP4 session has been released.

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 Ethernets 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/AMS and hence the DHCP Proxy/relay/server and FIAA entities are not involved in connection establishment. The mobility binding in case of Ethernets services contains the MS/AMS 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/AMS 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/AMS. 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 [93] 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/AMS MAC address.

The PMIP4 client SHALL support the GRE Key extension as defined in draft-yegani-gre-key-extension-03 [92]. When the PMIP4 client is triggered by the authenticator, it allocates a unique GRE key for the MS/AMS and saves it as part of the MS/AMS 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/AMS.

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.

The Registration Request message is protected with the MN-HA AE as described in section 4.8.2.1.3.

Upon receiving a MIP4 Registration Reply message from the Home Agent, the PMIP4 Client SHALL validate the message as described in section 4.8.2.1.3. If the message validation fails, the PMIP4 Client SHALL notify the collocated authenticator that the MIP4 authentication failed.

The PMIP4 client SHALL verify that the Registration Response indicating successful registration contains the GRE key extension. The PMIP4 client SHALL save the GRE key received from the HA as part of the MS/AMS context. If the Registration Response does not contain the GRE Key extension, the PMIP4 client SHALL inform the collocated authenticator that the R3 establishment failed.

The PMIP4 client SHALL verify that the Registration Response indicating successful registration contains the Proxy Mobile IPv4 Device ID Extension. The ID-Type in the Proxy Mobile IPv4 Device ID option MUST be set to 1 and the Identifier field MUST be set to the value of the MS/AMS MAC address that was included in the Registration Request message.

Upon receiving the Registration Response message with the Proxy Mobile IPv4 Device ID Extension included, the PMIP4 client SHALL ignore the Home address filed in the Registration Response message.

If the Proxy Mobile IPv4 Device ID extension is not included in the Registration Reply message, the PMIP4 client SHALL assume that the HA does not provide support for Ethernet services as described here and SHALL inform the authenticator that the R3 connection establishment was not successful. If the reply code in the Registration Reply message indicated successful registration, but the Proxy Mobile IPv4 Device ID extension was absent from the Registration Reply message, the PMIP4 client SHALL initiate the MIP4 de-registration as described in section 4.8.2.4.8.1.2.

4.8.2.5.1.3 FA Requirements

The FA SHALL operate as defined in section 4.8.2.1.3, with additional considerations as described in this section.

The FA SHALL support GRE encapsulation between the FA and the HA and it SHALL support the GRE key extension as defined in draft-yegani-gre-key-extension-03 [92].

When encapsulating the user plane traffic, the FA SHALL use the GRE key from the MS/AMS context to fill in the value of the GRE Key in the uplink packet.

When receiving the downlink traffic from the HA, the FA SHALL use the GRE key from the downlink packet to locate the MS/AMS to which this packet SHALL be delivered.

4.8.2.5.1.4 HA Requirements

The HA SHALL operate as described in section 4.8.2.1.3 and in this section.

The HA SHALL support GRE encapsulation between the FA and the HA and it SHALL support the GRE key extension as defined in draft-yegani-gre-key-extension-03.

The HA validates the Registration Request message and the MN-HA AE as described in section 4.8.2.1.3.

When the HA receives a Registration Request message containing the Proxy Mobile IPv4 Device ID Extension, the HA SHALL verify that the ID-Type in the Proxy Mobile IPv4 Device ID option is set to 1. It then extracts the MS/AMS MAC address from the identifier field of the Proxy Mobile IPv4 Device ID Extension and saves it as part of the MS/AMS context.

When the HA receives the Registration Request message with the GRE Key extension and if the message also contains the Proxy Mobile IPv4 Device ID Extension, the HA SHALL save the received GRE key as part of the MS/AMS context. The HA SHALL use the received GRE key for encapsulating the downlink traffic tunneled to the FA.

If the HA receives a Registration Request message where the Proxy Mobile IPv4 Device ID extension is included but the requested encapsulation method is not GRE or the GRE key extension is missing, the HA SHALL reject such Registration Request.

If the Registration Request message contains the Proxy Mobile IPv4 Device ID Extension the HA SHALL disregard the Home address filed in the Registration Request message and SHALL set the Home address filed in the Registration Response message to the ALL-ZERO-ONE-ADDR.

The HA protects the Registration Response message with the MN-HA AE as described in section 4.8.2.1.3.

When sending the Registration Response message, the HA SHALL include the Proxy Mobile IPv4 Device ID Extension and the GRE Key extension. The Proxy Mobile IPv4 Device ID Extension SHALL be set to the same value as in the corresponding Registration Request message. The HA SHALL generate the GRE key used to mark the uplink traffic and save it as part of the MS/AMS context. The HA SHALL set the GRE Key extension in the Registration Response message to the value of this GRE key.

4.8.2.5.1.5 AAA Server Requirements

The AAA server requirements and the interface between the HA and the AAA server are as described in the section 4.8.2.1.3. of the baseline specification.

4.8.2.5.2 Session Renewal for Ethernet Services

Session renewal for Ethernet service is as described in the Figure 4-141 in section 4.8.2.2 of the baseline stage 3 specification.

4.8.2.5.2.1 FA Requirements

If the Proxy Mobile IPv4 Device ID Extension and the GRE Key extension were included in the initial Registration Request message that created the mobility binding, then the FA SHALL include the Proxy Mobile IPv4 Device ID Extension and the GRE Key extension in every subsequent Registration Request message.

When extending the mobility binding, the FA SHALL include the same values for the MAC address and the GRE key in the Registration Request message that were used during the initial registration. The Home address field in the Registration Request is set to the same value as in the initial Registration Request message.

The rest of the FA requirements are the same as in the section 4.8.3.1.2 of this document.

4.8.2.5.2.2 HA Requirements

If the HA included the Proxy Mobile IPv4 Device ID Extension and the GRE Key extension in the initial Registration Response message when the mobility binding was created, then the HA SHALL include the Proxy Mobile IPv4 Device ID Extension and the GRE Key extension in every subsequent Registration Response message.

The Home address field in the Registration Response is set to the same value as in the initial Registration Response message.

The rest of the HA requirements are the same as in the section 4.8.3.1.3 of this document.

4.8.2.5.3 CSN-anchored Mobility Management Handover for MIP-based Ethernet Services

The procedures for CSN-anchored mobility management are as described in the section 4.8.2.3.8 of the stage 3 baseline document and as amended here.

The serving ASN SHALL include the Uplink R3 GRE key and Downlink R3 GRE key as part of the MIP4 Info provided to the Target ASN during the CSN-anchored handover.

The target ASN SHALL save the Uplink R3 GRE key and Downlink R3 GRE key as part of the MS/AMS context.

When the target ASN receives the Uplink R3 GRE key and Downlink R3 GRE keys during the MS/AMS handover, the target ASN SHALL use the GRE encapsulation on the R3 interface towards the HA.

When encapsulating the uplink traffic, the target ASN SHALL use the Uplink R3 GRE key to fill in the Key field in the GRE header.

When receiving the packet from the HA, the target ASN SHALL match the Downlink R3 GRE Key from the MS/AMS context with the GRE key from the packet header to determine the MS/AMS 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 4.8.2.4.8.1.2 (ASN Initiated PMIP4 Session Release), 4.8.2.4.8.1.3 (HA Initiated PMIP4 Session Release) and 4.8.2.4.8.1.4 (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/AMS. Likewise, the Registration Revocation Acknowledgment message SHALL contain the Proxy Mobile IPv4 Device ID Extension identifying the MS/AMS 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/AMS, and SHALL tunnel it to the current FA of the MS/AMS using GRE encapsulation.

The mobility binding of the MS/AMS 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/AMS 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/AMS 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/AMS Requirements

The Mobile IPv4 Client behavior assumes that the Mobility Stack in the MS/AMS conform to IETF standards such as [49].

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/AMS 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/AMS did not already request for an IP address using DHCP or FIAA. Otherwise, the MS/AMS SHALL not initiate CMIP4 registration procedure once it has received an IP address from the network via DHCP or FIAA. In the RRQ, the MS/AMS 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/AMS may use dynamic HA assignment and/or dynamic HoA address assignment. If the MS/AMS 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/AMS 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/AMS prefers an HA assignment in the home domain, while 0.0.0.0 means the MS/AMS has no preference for home vs. visited domain assignment.

The MS/AMS 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/AMS 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/AMS. The HoA MUST be updated with the assigned value once the RRP with success code is received.

MS/AMS 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/AMS 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).

The MN-FA Challenge Extension as specified in [43] is not supported.

The error handling and retransmission behavior of the MS/AMS SHALL be governed by the Mobile IPv4 standard [49].

When connected to a WiMAX network, if the MS/AMS wants to use CMIP4 it SHALL NOT invoke DHCP or FIAA for IPv4 address acquisition before and after starting the Mobile IP procedures.

The scenario when the MS/AMS performs CMIP4 registration after the network performs PMIP4 procedures is not in the scope of this Release. In other words, in this Release once the MS/AMS sends DHCPREQUEST or an FIAA IE with AAI_REG_REQ, it is not expected to follow it later on with MIP RRQ messages.

4.8.3.1.2 FA Requirements

FA and anchor DPF are always collocated. As soon as the FA (collocated with the DPF) determines that the data path (i.e., R6) is connected for a new MS/AMS for which no mobile IPv4 session exists, the FA SHALL send a series of Agent Advertisement over that data path (i.e., R6) to the MS/AMS after a configurable time period (to allow the MS/AMS to initiate either Simple IPv4 or CMIP4). The Agent Advertisement SHALL contain the FA-CoA and the supported lifetime. The FA SHALL set the MIP lifetime < AAA session time attribute value that the FA is configured to support. The Agent Advertisement SHALL be formatted as per [49] The FA SHALL support MIP4 registration revocation as per [51] and the FA SHALL set the appropriate fields in the Agent Advertisement message.

The FA SHALL send Agent Advertisement under the following conditions:

a. The DPF notifies the FA that the data path (i.e., R6) is up and the FA determines that the MS/AMS is authorized for only CMIP4 from the subscriber profile which may be cached in the NAS (received during user/device authentication from the HAAA).

b. The DPF in the target ASN forwards the Anchor DPF *HO_Req* received over R4 to the target FA. Note that the currently serving ASN is responsible for ensuring that the MS/AMS is a CMIP4 authorized MS/AMS and the MS/AMS has an active CMIP4 session. The target FA does not perform additional MS/AMS capability checks before sending Agent Advertisement.

c. When solicited by the MS/AMS unless the MS/AMS has an existing IPv4 session.

Upon receiving the RRQ message from the MS/AMS, with a static HA field, the FA SHALL relay the RRQ to the requested HA. If the HA field in the RRQ doesn't match the visited HA or the home HA address downloaded during access authentication, the FA SHALL reject the RRQ with an error code 136 (unknown home agent address). The MS/AMS may then retry using dynamic HA assignment.

If the MS/AMS has requested dynamic HA assignment by specifying the HA field as ALL-ZERO-ONE-ADDR, the FA SHALL relay the RRQ to the visited HA if there is visited HA address downloaded during access authentication AND if the HA field in the RRQ is all '0'. Otherwise, the FA relays the RRQ to the home HA address downloaded during access authentication.

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 (draft-leung-mip4-proxy-mode-05.txt) to indicate which access type is being used, before relaying the RRQ to the HA.

If GRE tunneling is used between the FA and the HA, the FA MAY include the GRE key extension CVSE carrying its GRE-key as defined in draft-yegani-gre-key-extension-03.txt.

Upon receiving the RRP back from the HA, the FA SHALL forward the RRP to the MS/AMS if FA-HA AE validation is successful (if FA-HA AE is used). If FA-HA AE is not used, the FA SHALL forward the RRP back to the MS/AMS.

The Registration Revocation message SHALL be either protected using an FA-HA Authentication Extension as per [51] or by using another security mechanism at least as secure, and agreed upon by the home and visited domains, e.g., IPsec. If an FA-HA security association is not available, or in the absence of another appropriate security mechanism, the FA and HA SHALL silently discard any Registration Revocation messages received.

If there is no alternative way to secure FA-HA communication other than FA-HA AE, the FA SHALL extract the 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 [49]. 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 RRPs 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 WHA4Acommand 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/AMS. 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/AMS if dynamic HoA assignment is requested (i.e., RRQ contains the HoA=0.0.0.0) and respond back to the MS/AMS 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 [51]. The generic error handling requirements for the HA are as per [49].

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/AMS 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/AMS incurring a handover to a target BS/ABS 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/AMS Requirements

A CMIP4 capable MS/AMS 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/ABS 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/AMS as soon as the data path to the MS/AMS is established.

Table 4-138 – 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	

IE	Reference	M/O	Notes
>>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.
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/AMS 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 4-120. The further processing of the resulting RRQ and RRP at the target FA for the MS/AMS is as per section 4.8.2.1.5.

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/AMS. 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/ABS. 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/ABS must update its notion of the location of the anchor DPF function for this MS/AMS. The serving BS/ABS 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/AMS to register its new CoA as per section 4.8.2.1.6. 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 [51] from the FA.

4.8.3.3.4 AAA Server Requirements

Same as section 4.8.2.1.7.

4.8.3.3.5 MS/AMS Mobility Triggered

For CMIP4 based CSN anchored Mobility Management, the MS/AMS 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/AMS 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 [51].

4.8.3.3.7 CMIP4 Mobility Procedure

4.8.3.3.7.1 CMIP4 CSN MM Handover

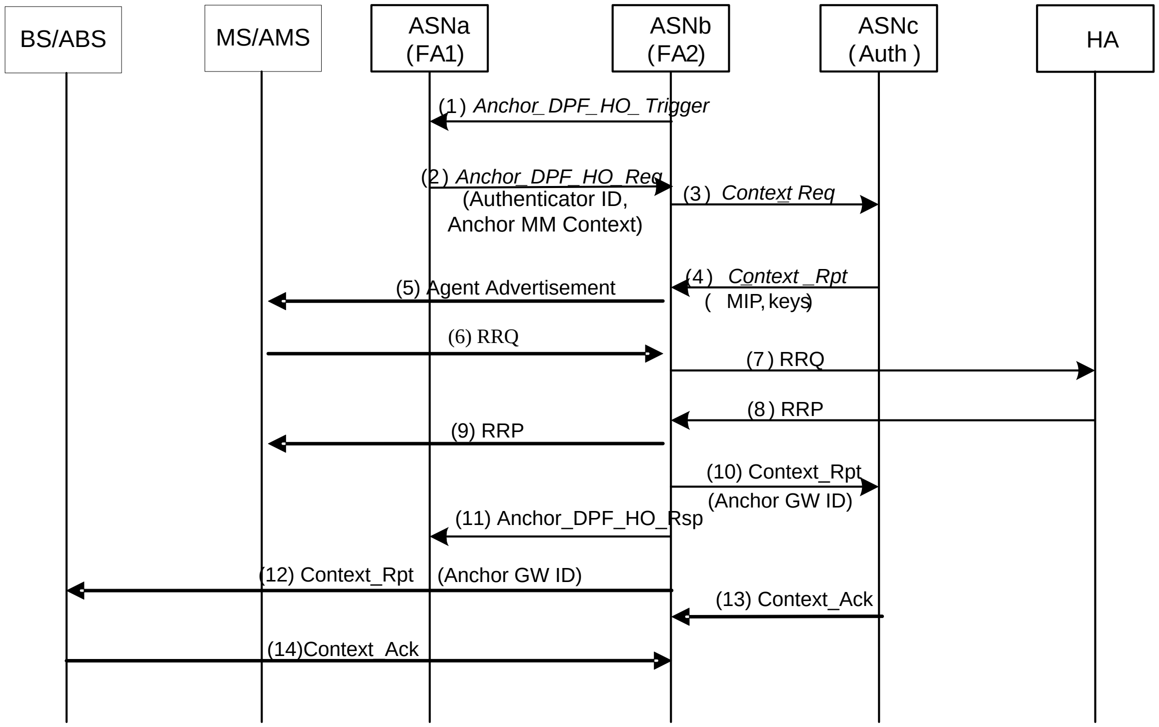

BS/ABS
MS/AMS
ASNa (FA1)
ASNb (FA2)
ASNc (Auth)
HA
(1) Anchor_DPF_HO_ Trigger
(2) Anchor_DPF_HO_Req (Authenticator ID, Anchor MM Context)
(3) Context Req
(4) Context _Rpt (MIP, keys)
(5) Agent Advertisement
(6) RRQ
(7) RRQ
(8) RRP
(9) RRP
(10) Context_Rpt (Anchor GW ID)
(11) Anchor_DPF_HO_Rsp
(12) Context_Rpt (Anchor GW ID)
(13) Context_Ack
(14)Context_Ack

Figure 4-149 – 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 4-119. 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/AMS and the Authenticator Id and ASNa will start a timer $T_{Anchor\_DPF\_HO\_Req}$[26] 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.

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/AMS.

STEP 6-9

The MS/AMS 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/AMS. At this point, ASNb gets registered with HA.

STEP 10

ASNb sends Context Report to the Authenticator GW. The Context_Rpt message contains the address of the new anchor DPF function.

STEP 11

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 12

ASNb sends Context Report to the BS/ABS. The Context_Rpt message contained the address of the new anchor DPF function.

[26] $T_{Anchor\_DPF\_HO\_Req}$ value should be larger than the sum of $T_{R4\_Cntxt\_Req}$ including retransmissions and time taken to register with HA.

STEP 13

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/AMS. The anchor authenticator confirms the receipt of the Context_Rpt message by sending the Context_Ack message.

STEP 14

BS/ABS also updates location of the anchor DPF function for this MS/AMS upon receipt of the Context_Rpt message. The BS/ABS 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 4-139 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-139 – Timer Values for CMIP4 CSN MM Handover Messages over R4/R3

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{Anchor\_DPF\_HO\_Trigger}$	TBD		TBD
$T_{Anchor\_DPF\_HO\_Req}$	TBD		TBD
$T_{R4\_Cntxt\_Req}$	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 4-140 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 4-140 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{Anchor\_DPF\_HO\_Trigger}$	Target FA	CMIP4 CSN MM handover is aborted and further action of Serving/Target FA is implementation Specific.
$T_{Anchor\_DPF\_HO\_Req}$	Serving FA	CMIP4 CSN MM handover is aborted and further action of Serving/Target FA is

		implementation Specific.
T $_{R4\_Cntxt\_Req}$	Target FA	CMIP4 CSN MM handover is aborted and *Anchor_DPF_HO_Rsp* 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/AMS MAY be either terminated by the MS/AMS 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/AMS Requirements

A CMIP4 capable MS/AMS 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/AMS has an ongoing Mobile IPv4 session) containing sequence number = 0, the MS/AMS SHALL consider its Mobile Ipv4 session terminated by the network. Moreover, if the Agent Advertisement has the B-bit set, the MS/AMS 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/AMS. The FA SHALL forward the RRP back to the MS/AMS if the corresponding R6/R4 still exists.

The FA implementations compliant to this document SHALL support and use Mobile IPv4 Registration Revocation [51].

Based on what the I-bit setting in the Revocation Support Extension (sec 3.2, [51]) and the availability of R6 after registration revocation messages are exchanged with the HA, the FA MAY send an Agent Advertisement to the MS/AMS 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/AMS, the HA SHALL remove the mobility binding for the MS/AMS and reply with a RRP as per the behavior defined in [49].

The HA implementations compliant to this document SHALL support and use Mobile IPv4 Registration Revocation [51].

Upon receiving a Registration Revocation from the FA for an MS/AMS, the HA SHALL tear down the mobility binding state for the MS/AMS (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/AMS' 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/AMS 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/AMS.

4.8.4 Client MIP6 Mobility Management

Mobile IPv6 (MIP6) operation is specified by the IETF. The base specifications for MIP6 include RFCs [58]. As per [58] 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/AMS (Mobile Station) to the HA is via the Authentication protocol [72].

The MS/AMS 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:

- [58]: Base MIP6 protocol
- [72]: Authentication Protocol for MIP6
- [70]: Identification Option for MIP6
- [70]: draft-ietf-mip6-hiopt-12.txt
- [85]: 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/AMS triggers the registration procedure (connection setup) with the home agent. The decision to initiate MIP6 signaling by an MS/AMS to an HA is based on local policy at the host. The following sections define the node behavior of a MIP6 MS/AMS.

The MIP6 capable MS/AMS 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/AMS has to be bootstrapped with this information. The MS/AMS acquires the information required for establishing a MIP6 session via DHCPv6 or FIAA. Prior to the MS/AMS initiating DHCPv6 or FIAA, it has authenticated itself to the network via EAP. As part of the EAP transaction, the home AAA determines that the MS/AMS/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 using DHCP is as shown in Figure 4-150:

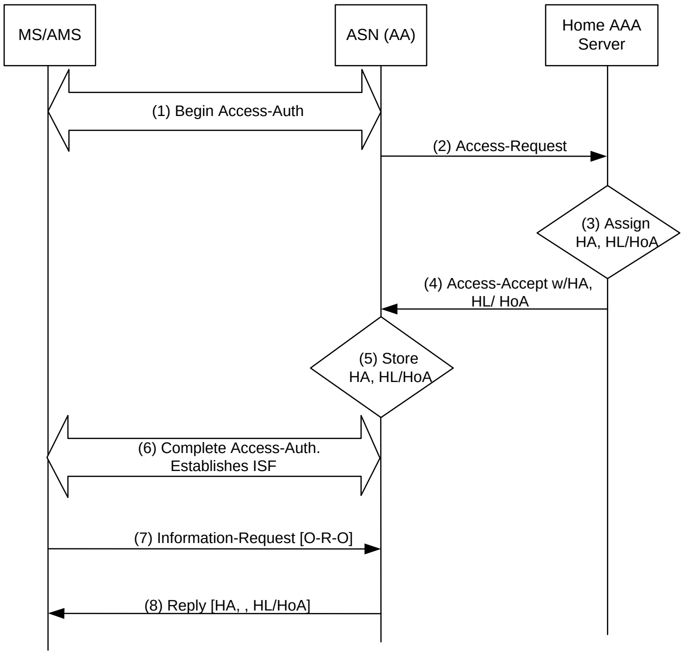


Figure 4-150 – Client MIP6 Connection Setup Procedure using DHCP

STEP 1

The MS/AMS 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/AMS.

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/AMS configures its IPv6 stack with a link local and global address as per the basic IPv6 connection setup procedure.

STEP 7

The MS/AMS requests the MIP6 bootstrap information using the DHCPv6 Information-request message [56] 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/AMS [56] with the options that were requested and attaches the MIP6 bootstrap information options as per draft-ietf-mip6-hiopt-12.txt [89].

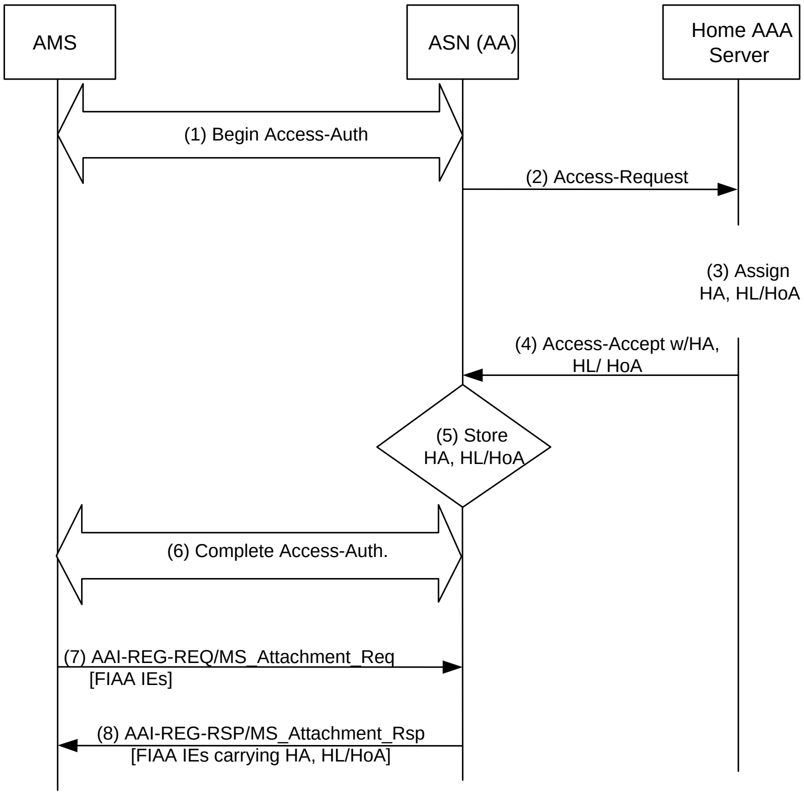

AMS
ASN (AA)
Home AAA Server
(1) Begin Access-Auth
(2) Access-Request
(3) Assign HA, HL/HoA
(4) Access-Accept w/HA, HL/ HoA
(5) Store HA, HL/HoA
(6) Complete Access-Auth.
(7) AAI-REG-REQ/MS_Attachment_Req [FIAA IEs]
(8) AAI-REG-RSP/MS_Attachment_Rsp [FIAA IEs carrying HA, HL/HoA]

Figure 4-151 – Client MIP6 Connection Setup Procedure using FIAA

STEP 1

The AMS 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 FIAA function.

STEP 6

The Access Authentication procedure completes successfully.

STEP 7

The AMS requests the MIP6 bootstrap information using the FIAA procedure. The Host-Configuration-Capability-Indicator is set to 1 and the Requested-Host-Configurations IE is included in the AAI-REG-REQ sent to the ASN.

STEP 8

The ASN responds with the with AAI-REG-RSP including FIAA IEs populated with the values obtained from AAA procedures (Home Agent Address, Home Address, Home Link Prefix).

4.8.4.1.1 MS/CMIP6 Client Operation

MIP6 is an integral part of the IPv6 stack in the MS/AMS. The terms MS/AMS 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/AMS configures (either via DHCPv6 or via auto-configuration) a global scope IPv6 address when attached to the ASN. Local policy at the MS/AMS 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.

When DHCP is used, the MS/AMS may discover 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/AMS to the DHCPv6 proxy or relay in the ASN. In the DHCP Information Request, the MS/AMS 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/AMS SHALL set the id-type to 1 in this option and include the @realm part of its NAI in the Home Network Identifier field. When FIAA is used, the same DHCP options are carried in Requested-Host-Configurations IE over AAI-REG-REQ sent by the AMS.

After obtaining the HA address via DHCP or FIAA (when they are used), 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 [72]. The MS/AMS 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/AMS SHALL include Mobile Node Identifier Option for Mobile IPv6 [70] 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/AMS also received the HoA in the DHCP Reply message, the MS/AMS SHALL set the HoA field in the BU to the received HoA.

If the MS/AMS did not receive the HoA via DHCP or FIAA but it received the HL prefix info, the MS/AMS can perform stateless address auto-configuration of the HoA from the received HL prefix as per autoconfiguration process described in [79]. In this case, the MS/AMS SHALL set the HoA field in the BU to the auto-configured HoA.

If the MS/AMS did not receive the HoA and HL prefix via DHCP or FIAA, the MS/AMS SHALL either set the HoA 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 Interface ID (IID) in the HoA field. In the latter case, the MS/AMS is requesting the HA to assign a HoA using the IID supplied by the MS/AMS. The MS/AMS SHALL perform back processing as per [72]. The MIP6 Route optimization feature requires the existence of an IPsec SA between the MS/AMS and the HA. Since the Authentication protocol is used for securing the registration messages, route optimization as described in [58] cannot be performed. Route optimization, in the scenario when the MS/AMS is using [72] for securing the CMIP6 registration messages, is for further study.

4.8.4.1.2 NAS and DHCPv6 Proxy Requirements

The NAS in the ASN, is also the Anchor Authenticator and should cache the Mobile IPv6 bootstrap parameters that are received from the Home AAA server at the time of Device/User Network Access Authentication and Authorization procedure. When using DHCP, upon receiving DHCPv6 information request from the MS/AMS the DHCPv6 proxy SHALL reply to the MS/AMS with the Home Network Information option with the MIP6 bootstrap info that was received from the AAA server. When using FIAA, the same DHCP option is delivered via the FIAA IEs over AAI-REG-RSP. To identify the set of information to convey to the MS/AMS, the DHCPv6 proxy and FIAA function SHALL use the R6 Path_ID to determine the set of cached parameters that is relevant to the MS/AMS. The DHCPv6 proxy and FIAA function may also receive the Home Network Identifier Option [89] in the DHCPv6 Information Request. However, the DHCPv6 proxy and FIAA function are not required to process this information. To convey the Home Agent address to the MS/AMS, the DHCPv6 proxy and FIAA function SHALL set the hainfo-type to 1 and the Home Network Information field to the Complete IPv6 address of the home agent in the Home Network Information Option. To indicate the received HL prefix, the DHCPv6 proxy or FIAA function SHALL set the hainfo-type to 0 and the Home Network Information field to Home subnet prefix in the Home Network Information Option. If both HA and HL prefix information need to be conveyed to the MS/AMS, the DHCPv6 proxy or FIAA function SHALL include two Home Network Information Options with fields set as described above.

4.8.4.1.3 HA Requirements

The HA SHALL support Mobile IPv6 operation with Base Mobile IPv6 [58] and Authentication Protocol for Mobile IPv6 [72]. Upon receiving a BU from a MS/AMS, the HA SHALL perform validation of MN-HA Mobility Message Authentication Option based on the identification of the user from the NAI contained in the BU in the Mobile Node Identifier Option [70] and the corresponding MN-HA key. The HA acquires the MN-HA key from the AAA by sending a RADIUS Access-Request packet or Diameter WHA6R command as shown in Table 5-8/Table 5-44. The User-Name attribute value is obtained from the NAI contained in the BU in the Mobile Identifier Option [70]. This NAI SHALL be the same NAI used as the Outer-Identity during Device/User Network Access Authentication and Authorization procedures. The HA SHALL also include the following attributes/AVPs: the IPv6 address of the HA so that the HAAA can validate that the correct values have been used. The HA SHALL sign the RADIUS packet using Message-Authenticator as specified in [53].

If the HA requires the Chargeable User Identity (CUI) attribute, it SHALL include the CUI attribute/AVP set to NULL in the RADIUS Access-Request packet or Diameter WHA6R command.

The HA SHALL include the WiMAX-Capability attribute/AVP indicating its capabilities to the HAAA.

Upon successful processing by the HAAA, the HA receives a RADIUS Access-Accept packet as shown in Table 5-8 or a Diameter WHA6A command as shown in Table 5-45. The HA SHALL validate the RADIUS Message-Authenticator as per the procedures defined in [53]. If the RADIUS packet does not contain the Message-Authenticator, the HA SHALL silently discard the packet. If the packet contains the Message Authenticator but the computed value does not match the Message Authenticator, then the HA SHALL silently discard the packet. If the

HA discards the RADIUS Access-Accept packet it should also discard the BU message. If the RADIUS validation is successful, then the HA should decrypt the MN-HA attribute using the procedures defined in [40] section 3.5.

Once the MN-HA key is obtained, the HA can validate the MN-HA AE. If the MN-HA AE is verified successfully, the HA SHALL create a security association with the MN storing the MN-HA key locally. The HA SHALL use the MN-HA key to compute MN-HA AE for all subsequent messages. Once the MN-HA AE is validated the HA SHALL continue to process the BU as prescribed below:

- If the MN-HA AE fails authentication, the HA SHALL silently discard the BU.
- If the RADIUS Access-Accept packet or Diameter WHA6A command contains MIP-Authorization-Status set to False, then MIP6 service is not authorized for the subscriber. The HA SHALL construct a BA with status set to Administratively prohibited (129). The BA SHALL include the MN-HA AE which is signed by the MN-HA key received in the RADIUS Access-Accept packet or Diameter WHA6A command.
- If the HA receives the CUI attribute in the RADIUS Access-Accept packet or Diameter WHA6A command, it SHALL include it in all RADIUS/Diameter accounting packets only if it supports accounting message as indicated by the WiMAX-Capability attribute sent in the RADIUS Access-Request packet or Diameter WHA6R command, and if accounting messages were selected by the RADIUS/Diameter server in the WiMAX-Capability attribute. Similarly, if accounting is enabled and the Class attribute is received in the RADIUS Access-Accept packet/Diameter WHA6A command, the HA SHALL include the Class attribute in all accounting messages.
- If the HoA contained in the BU is unknown to the HA but the prefix of the HoA matches one of the prefixes that the HA supports for HoA construction, the HA will assume that the MS/AMS discovered the HL prefix info via bootstrapping. In this case, the HA may perform a local check in the local repository of Binding Cache Entries (BCEs) to make sure that the address (HoA) does not clash with that of another mobility binding. The HA SHALL perform the uniqueness validation of the assigned or requested HoA as per [58]. If the uniqueness of the HoA validation succeeds, the HA admits the binding and replies to the MS/AMS with a BA. The BA is protected by the MN-HA Mobility Message Authentication Option.
- If the HoA contained in the BU contains 0::0 (unspecified address) or EUI-64/IID the HA SHALL consider this as a request for a dynamic HoA assignment request from the MS/AMS. In the former case, the HA SHALL assign a 128-bit IPv6 address (HoA) from its local repository for the MS/AMS. In the latter case, the HA SHALL auto-configure a HoA with the received IID and a shared /64 prefix. In this document it is assumed that the /64 prefix is solely owned by the HA (i.e., no other HA owns and uses that prefix). HA SHALL make sure by checking in the local repository of BCEs that the auto-configured HoA does not clash with another HoA that is being used by some other user. If for some reason the HA finds a clash, the HA SHALL use either a globally unique /64 prefix to auto-configure the HoA or it SHALL use a shared /64 prefix to do the same. In the latter case, the HA SHALL again perform the BCE check to detect any clash. When the HA determines that the HoA assigned or auto-configured for the MS/AMS is unique, the HA SHALL admit the mobility binding for the MS/AMS with that HoA.
- If the HA receives Prepaid attributes/AVPs in the RADIUS Access-Accept packet or Diameter WHA6R command then it SHALL proceed to perform the prepaid procedures as specified in section 4.4.3.3.
- If the HA receives Hot-lining attributes/AVPs in the RADIUS Access-Accept packet or Diameter WHA6R command then it SHALL proceed to perform the hot-lining procedures as specified in section 4.4.3.5.
- If the HA supports accounting and the RADIUS/Diameter server requested accounting for this user, the HA SHALL send a RADIUS Accounting-Request Start with Session Begin set to TRUE or a Diameter WACR command with Accounting-Record-Type set to START_RECORD as described in the Accounting session indicating that the Session has started.

Given the particular (HA) deployment assumptions for WiMAX Rel.1 the MS/AMS is always away from its home IP link and hence the HA is in a virtual home.

4.8.4.1.4 AAA Requirements and Behavior

The HA interfaces with the HAAA server in the CSN.

During Device/User Network Access Authentication and Authorization procedures, the HAAA sends MIP6 bootstrap information to the ASN (NAS, DHCPv6 Proxy, and FIAA function) as specified in Section 4.1.

When the HA receives a BU from the MS/AMS, the HA constructs a RADIUS Access-Request packet or Diameter WHA6R command to fetch the MN-HA key which is needed for authenticating the BU. The RADIUS Access-Request packet is shown in Table 5-8. The Diameter WHA6R command is shown in Table 5-44.

During routing operations the VAAA SHALL process the NAI found in the User-Name attribute as specified by [69] 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.

The HAAA SHALL validate the Message-Authenticator in the RADIUS Access-Request packet as per procedures defined in [53]. If the message does not contain the Message Authenticator, or if the Message-Authenticator validation fails, then the HAAA SHALL silently discard the packet.

The User-Name AVP SHALL contain the Identity@realm that was used (pseudo or real) during Device/User Network Access Authentication and Authorization procedures. The AAA SHALL locate the Identity and ensure that it matches an internal identity. If PseudoIdentity was used and cannot be found, then the HAAA SHALL reply back with an RADIUS Access-Reject packet or Diameter WHA6R command with the error code indicating missing User-Name AVP.

If the pseudo Identity is found then the HAAA SHALL reply with a RADIUS Access-Accept packet as shown in *Table xx2* containing the MN-HA key encrypted using the procedures defined in [40] section 3.5 or Diameter WHA6R command containing the MN-HA key. The RADIUS packet SHALL include the Message-Authenticator computed according to [53].

If the HAAA determines that the user is not authorized for MIP6 then it SHALL set the value of the MIP-Authorization-Status to False. Otherwise if the user is authorized for MIP6 service, the HAAA SHALL set the MIP-Authorization-Status to True.

If the RADIUS Access-Request packet or Diameter WHA6R command contains the CUI attribute set to NULL, then the HAAA SHALL also include the CUI computed using the procedures defined in section 4.4.3 in the RADIUS Access-Accept packet or Diameter WHA6A command.

If the User is a prepaid user and prepaid is to be performed at the HA (providing the HA indicated it supports Prepaid Capabilities in the WiMAX-Capability Attribute/AVPs), then the HAAA SHALL include prepaid attributes in the RADIUS Access-Accept packet or Diameter WHA6A command as specified in section 4.4.3.3.

If the MS/AMS is to be hot-lined, and the hot-lining is to be performed at the HA (provided the HA is capable of supporting hot-lining as indicated in the WiMAX-Capabilities Attribute/AVP), then the HAAA SHALL include the hot-lining attributes as specified in section 4.4.3.5.

4.8.4.2 MIP6 Inter Access Router (AR) Handovers

An ongoing session by an MS/AMS that is using CMIP6 may incur an inter Access Router handover. This may happen due to the MS/AMS incurring handover to a BS/ABS that has connectivity to a new Access Router or the serving ASN Functional Entity may decide to force a handover due to resource management reason or administrative reasons. The following sections detail the operation of such handovers.

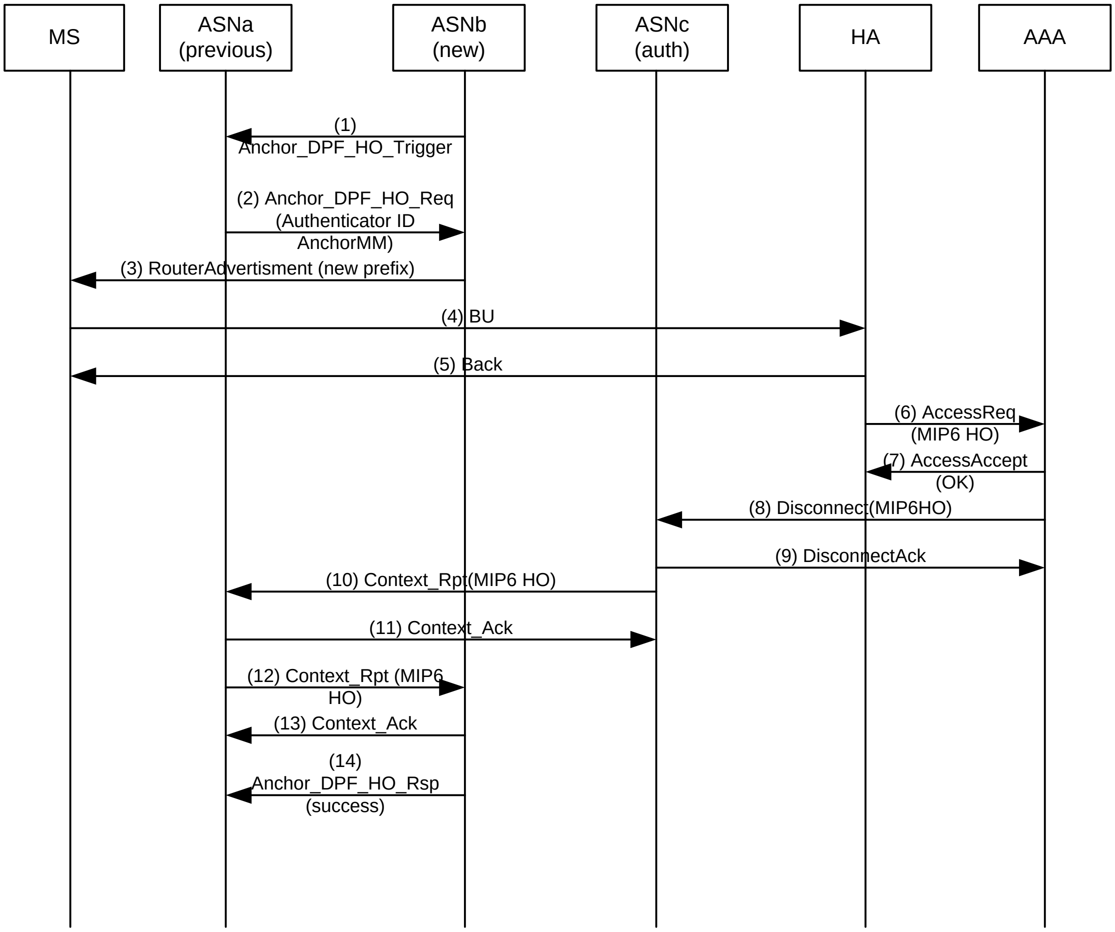

MS
ASNa (previous)
ASNb (new)
ASNc (auth)
HA
AAA
(1) Anchor_DPF_HO_Trigger
(2) Anchor_DPF_HO_Req (Authenticator ID AnchorMM)
(3) RouterAdvertisment (new prefix)
(4) BU
(5) Back
(6) AccessReq (MIP6 HO)
(7) AccessAccept (OK)
(8) Disconnect(MIP6HO)
(9) DisconnectAck
(10) Context_Rpt(MIP6 HO)
(11) Context_Ack
(12) Context_Rpt (MIP6 HO)
(13) Context_Ack
(14) Anchor_DPF_HO_Rsp (success)

Figure 4-152 – 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_Trigge*r, ASNb starts the timer $T_{Anchor\_DPF\_HO\_Trigger}$ for Anchor_DPF_HO_Req. Once Anchor_DPF_HO_Req, indicating the anchor DPF relocation decision of ASNa, is received by ASNb, $T_{Anchor\_DPF\_HO\_Trigger}$ 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/AMS, and ASNa will start a timer $T_{Anchor\_DPF\_HO\_Req}$ for *Anchor_DPF_HO_Rsp* from ASNb.

STEP 3

Target ASN for anchor DPF relocation sends a Router Advertisement message to the MS/AMS containing a new prefix used by the MS/AMS to formulate a new CoA.

STEP 4

After the MS/AMS 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/AMS 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/AMS 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/AMS 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/AMS.

4.8.4.2.1 MS/AMS/ CMIP6 Client Operation

The MS/AMS/ CMIP6 Client SHALL reset its MIP6 binding with a CoA as soon as the MS/AMS 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/AMS SHALL perform IPv6 connectivity negotiation as defined in section 4.11.3. In case of stateful IPv6 address configuration scenario for CoA with DHCPv6 or FIAA, the MS/AMS won't be able to send and receive any data unless it reconfigures the IPv6 stack with a new CoA via DHCPv6 or FIAA. This is because the target AR may not be able to support the CoA that the MS/AMS 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/AMS SHALL perform Mobile IPv6 BU/BA procedures. However, since it is an ongoing Mobile IPv6 session, the MS/AMS does not need to acquire the MIP6 bootstrap information from the target NAS. Also, the MS/AMS 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/AMS 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/AMS bootstrap the MIP6 parameters in case, the MS/AMS' 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/AMS movement.

The serving AR SHALL receive a Context_Rpt message from the authenticator indicating that MS/AMS 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/AMS. 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/ABS. 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/ABS must update its notion of the location of the anchor DPF function for this MS/AMS. The serving BS/ABS 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/AMS 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/AMS with remaining lifetime of the ongoing MIP6 session.

After updating the mobility binding for the MS/AMS 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/AMS 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/AMS 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/AMS 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/AMS/ CMIP6 Client Requirements

The MS/AMS SHALL send a Binding Update to the HA if it wishes to continue the IPv6 mobility session. The MS/AMS 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/AMS before expiry of the mobility session lifetime. In response, the HA SHALL send back a BA to the MS/AMS 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/AMS 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/AMS/ CMIP6 Client Requirements

The MS/AMS SHALL send a BU to the HA with lifetime set to 0 if it wishes to terminate the IPv6 mobility session. The MS/AMS SHALL construct the BU as per the details described in 5.6.3.2.1. After receiving the corresponding BA, the MS/AMS SHALL tear down the IPv6 session if MIP6 was the only session for the MS/AMS.

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/AMS. The AR (the serving DPF) may be able to inspect the BU/BAs that the MS/AMS 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/AMS if the MS/AMS 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/AMS with lifetime = 0. In response, the HA SHALL send back a BA to the MS/AMS 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 WACR 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/AMS 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 [72] (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/AMS.

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/AMS 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 [72] 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/AMS. 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 [72] 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/AMS 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/AMS upon an R3 handover.

When the negotiated mechanism is the lower-layer security, then the MAG/LMA SHALL not include Mobility Message Authentication Option [72] 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 [72] specification is originally written for RFC 3775 CMIP6 protocol [58]. Reference [72] also applies to PMIP6 [82] since PMIP6 is based on CMIP6. In order to apply [72] to PMIP6 (RFC5213) [82], a mapping profile is needed as the terminology in [72] is specific to CMIP6 [58]. Reference [72] SHALL be used in accordance with the following table as it gets implemented for securing PMIP6.

Table 4-141 – 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 [56]	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 [72])	Use the value of "PCoA" (MAG's IPv6 address)
"home address" value used in hash computation (Section 5.1 of [72])	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/AMS, 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 [94].

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 by setting bit #1 (Mobility support for IPv6) in PMIP6-Service-Info attribute of the RADIUS Access-Request respectively Diameter WDER. 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 or Diameter WDEA 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.

At the time of network access authentication, the ASN (NAS) SHALL include PMIP6 Service Info attribute when it sends the RADIUS Access-Request or Diameter WDER to HAAA. For dual IPv4/v6 service, the dedicated AAA attribute of PMIP6 Service Info will be used as follows:

- The ASN which is able to accommodate mobility management for dual IPv4/v6 hosts SHALL indicate this capability by setting bit #1 (Mobility support for IPv6) and by setting bit #2 (Mobility support for IPv4) to value 1.

Depending on the subscriber profile, network configuration policy, etc. the HAAA responds with RADIUS Access-Accept or Diameter WDEA using the same bits in PMIP6 Service Info attribute by setting bit #1 (Mobility support for IPv6) and by setting bit #2 to value 1 (Mobility support for IPv4).

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 [95] and Table 5-57, otherwise one of the IPv4 encapsulation modes specified in [94] 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/AMS. 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/AMS'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/AMS undergoes. For an IPv6 MS/AMS the WiMAX network SHOULD provide both stateful (DHCP and FIAA) and stateless address (auto)configuration modes with per-MS/AMS unique prefix assignment, while for IPv4 MS/AMS's PMIP6 procedure, the DHCPv4 and FIAA support are needed to distribute the IPv4 MN-HoA to the MS/AMS.

4.8.5.3.1 MS/AMS Requirements

The MS/AMS 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/AMS SHALL act according to the information received from the AR/MAG in the (un)solicited Router Advertisement message. The address on MS/AMS's network interface is configured either by stateless address autoconfiguration or through stateful DHCPv6 or FIAA configuration procedure following guidelines defined in section 4.11.4. The IPv6 address the MS/AMS configures for itself is in PMIP6 terms referred to as MN-HoA.

The IPv4 MS/AMS SHALL use the DHCPv4 protocol or FIAA 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.
- The NAS SHALL explicitly inform the AAA of the IP transport and mobility abilities in scope of PMIP6 by including the indications in the PMIP6-Service-Info attribute: bit for lower-layer transport security is set (when such support is in place), mobility management for IPv4 and IPv6 hosts is indicated when supported by the ASN, and IPv4 backhaul support is indicated when present.
- When MS/AMS attaches through a visited network, the VCSN SHALL indicate its PMIP6 support, i.e., the LMA & DHCP capabilities, if those are available by adding the corresponding indications in the VCSN Network Capability TLV and other related attributes as part of the Access-Request message.
- If the HAAA acknowledges PMIP6 as an authorized IP service, it SHALL deliver the related PMIP6 subscriber/service profile information in the AAA Access-Accept message sent to the ASN and VCSN. The profile MUST provide the following information:
    - PMIP6 listed under Authorized IP Network or Visited Authorized Network Services.
    - Address of the home- and/or visited LMA designated for that specific MS/AMS's IP session. When IPv4 transport is to be used over R3, the IPv4 address of the home- or visited-LMA has to be present.
    - If available at the HAAA, the IPv6 Home Network Prefix (HNP) or the IPv4 MN-HoA. Both configuration options may be present in the HAAA response.
    - When DHCP service for PMIP6 is authorized, information associated with the DHCP Proxy/Relay functions e.g., the DHCPv4/v6 server address, DHCP security parameters, etc.
    - Authorization of host IP mobility type (IPv6 and/or IPv4 bit SHALL be set in responding the PMIP6-Service-Info attribute)
    - Directive on PMIP6 signaling protection method to be applied (lower-layer or in-band protocol security bits in the PMIP6-Service-Info attribute)
    - Security bootstrapping parameters (PMIP6 root key and the associated SPI)
- The NAS/Authenticator SHALL store the obtained information locally and keep it available to the corresponding PMIP6 mobility entities in the ASN (MAG, DHCP function, etc.) throughout the IP session lifetime.

During routing operations the VAAA SHALL process the NAI found in the User-Name attribute as specified by [69] 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.

4.8.5.3.3 AR/MAG Requirements

The AR/MAG MUST obtain the Home Network Prefix (or IPv4 Home Address) before sending the first Router Advertisement or proceeding with DHCP/FIAA message exchange. The means to allocate HNP/HoA include bootstrapping from the AAA server, or assignment by the LMA via PBU-PBA exchange.

The PMIP6 IP mobility management for the attaching MS/AMS is authorized on per-MS/AMS basis by the HAAA appending the appropriate authorization hint in the Access-Accepts PMIP6-Service-Info attribute. Bit #1 is set if assignment and mobility of IPv6 address/prefix is authorized for the MS/AMS, bit #2 is set when mobility with an IPv4 address is allowed. The AR/MAG SHALL act corresponding to the mobility type authorization when constructing the PBU message: if both mobility types are authorized, the PBU SHOULD include both HNP and IPv4 Home Address mobility options. For constructing the PBU and processing PBA response from the LMA, the AR/MAG SHALL follow requirements from [82] on MS/AMS attachment and initial binding registration, and receiving the PBA, with one key difference. Inline with PMIP6 service authorization results from the Access-Accept, the AR/MAG MUST apply in-band protocol security to the PBU sent to the LMA. When lower-layer transport security is only requested by the HCSN, AR/MAG will abandon explicit protection of PMIP6 control plane.

The initial PBU SHALL be formed in accordance with guidelines in section 5.7, and needs to contain valid MN identifier information, HO indicator option with value set to attach over a new interface (HOI=1), the Access Technology Type (ATT) option with value set to 5 to indicate WiMAX access, the link-local address option, and the Timestamp mobility option. The HNP and IPv4 HoA mobility options will be populated in the PBU if the information was obtained prior from the AAA server. The remaining PBU fields and mobility options are composed as defined in Table 5-57.

When IPv4 support in PMIP6 is utilized, the AR/MAG SHALL operate as specified in [82]. 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/AMS'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/AMS corresponding to the address configuration mode associated with the MS/AMS's IP session; "A" flag is set in the Prefix Information Option if the MS/AMS 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/AMS 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. If the AMS chooses to use FIAA during the network entry procedure, then neither DHCPv6 nor stateless address autoconfiguration methods are used subsequently.

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/AMS, 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/AMS'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/AMS 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/AMS as a hint for the DHCP Server.

4.8.5.3.5 FIAA Requirements

The FIAA function entity learns the AMS' addressing information (i.e., HNP or IPv4 MN-HoA) either from the NAS or the AR/MAG. The NAS SHALL provide the HNP/MN-HoA to the FIAA 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 ASN MUST delay responding to MS_Attachment_Req until the initial binding registration for the AMS is completed and a BCE is established.

4.8.5.3.6 LMA Requirements

The LMA SHALL support relevant PMIP6 AAA attributes defined in section 5.4.3 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 [82]. 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 5-57.

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 [82]. If the R3 reference point is completely IPv4-based, the LMA MUST accept registration of IPv4 Proxy CoA to MS/AMS's BCE. The LMA SHOULD verify the PMIP6 mobility management for the attaching IPv4 MS/AMS 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/AMS 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/AMS with the MN ID and HNP/HoA it received. The LMA SHALL allow simultaneous registration of IPv4 MN-HoA and HNP for the MS/AMS 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/AMS, 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/AMS. If a GRE Key option [95] 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.

4.8.5.3.7 PMIP6 Connection Setup flows

4.8.5.3.7.1 Stateful DHCPv6 connection setup

Figure 4-153 presents PMIP6 connection setup procedure through stateful DHCPv6 address configuration according to the MS/AMS 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.

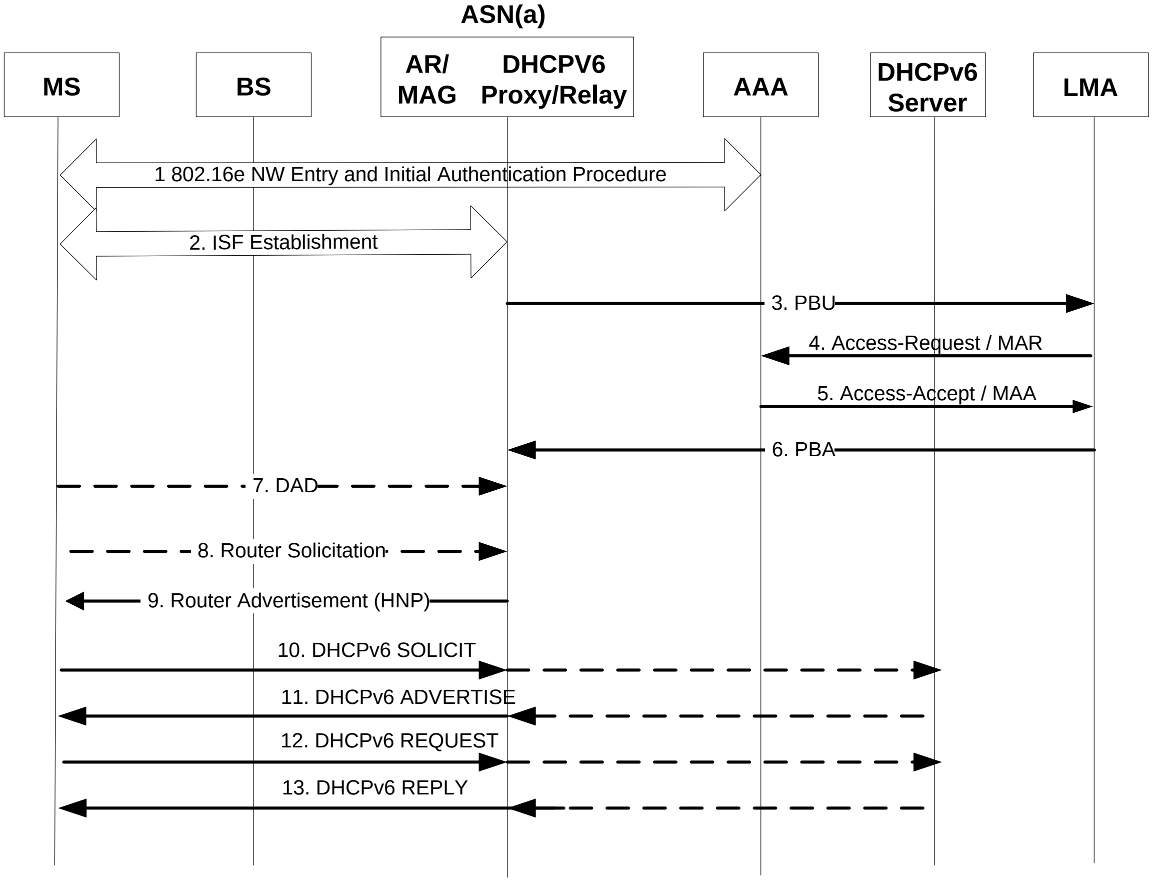


Figure 4-153 - PMIP6 connection setup procedure through DHCPv6

STEP 1

MS/AMS 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/AMS.

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/AMS'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/AMS's uplink and downlink payload forwarding. The PBA includes the MS/AMS'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/AMS configures a link local address, and MAY start a duplicate address detection process to verify it.

STEP 8

MS/AMS 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/AMS 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/AMS 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/AMS.
- 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/AMS.

STEP 12

The MS/AMS 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/AMS 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/AMS'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/AMS.

After this step the MS/AMS MAY initiate request for an IPv4 HoA assignment if such service is authorized and supported by the network.

4.8.5.3.7.2 Stateless address autoconfiguration connection setup

Figure 4-154 presents PMIP6 connection setup based on IPv6 stateless address autoconfiguration procedure.

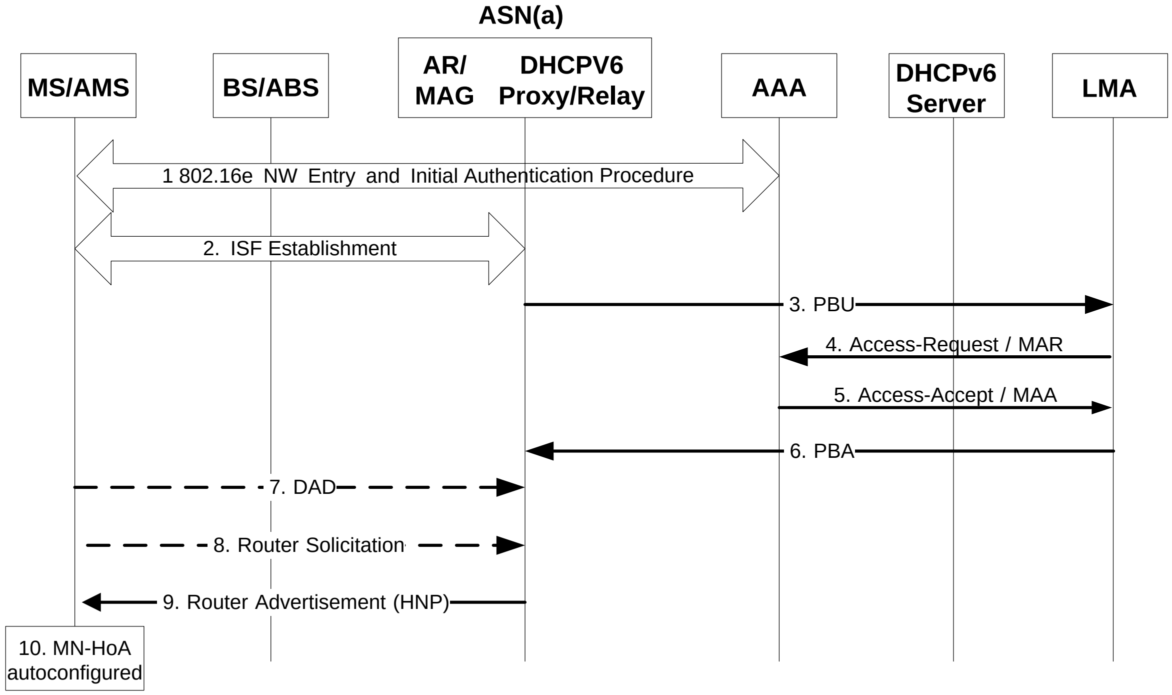


Figure 4-154 - PMIP6 connection setup procedure with SLAAC

STEP 1

MS/AMS 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/AMS.

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/AMS 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/AMS 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/AMS 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/AMS configures the link local address, and may start the duplicate address detection process.

STEP 8

MS/AMS 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/AMS. The Router Advertisement message with the “A” flag set contains per-MS/AMS unique prefix HNP/64 which allows the MS/AMS to directly autoconfigure its PMIP6 MN-HoA.

STEP 10

The MS/AMS configures a globally routable IPv6 address using the stateless autoconfiguration process. The MS/AMS 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/AMS MAY initiate request for an IPv4 HoA assignment if such service is authorized and supported by the network.

4.8.5.3.7.3 Connection setup for IPv4 using DHCP

Figure 4-155 shows the connection setup procedure via PMIP6 for an IPv4 MS/AMS:

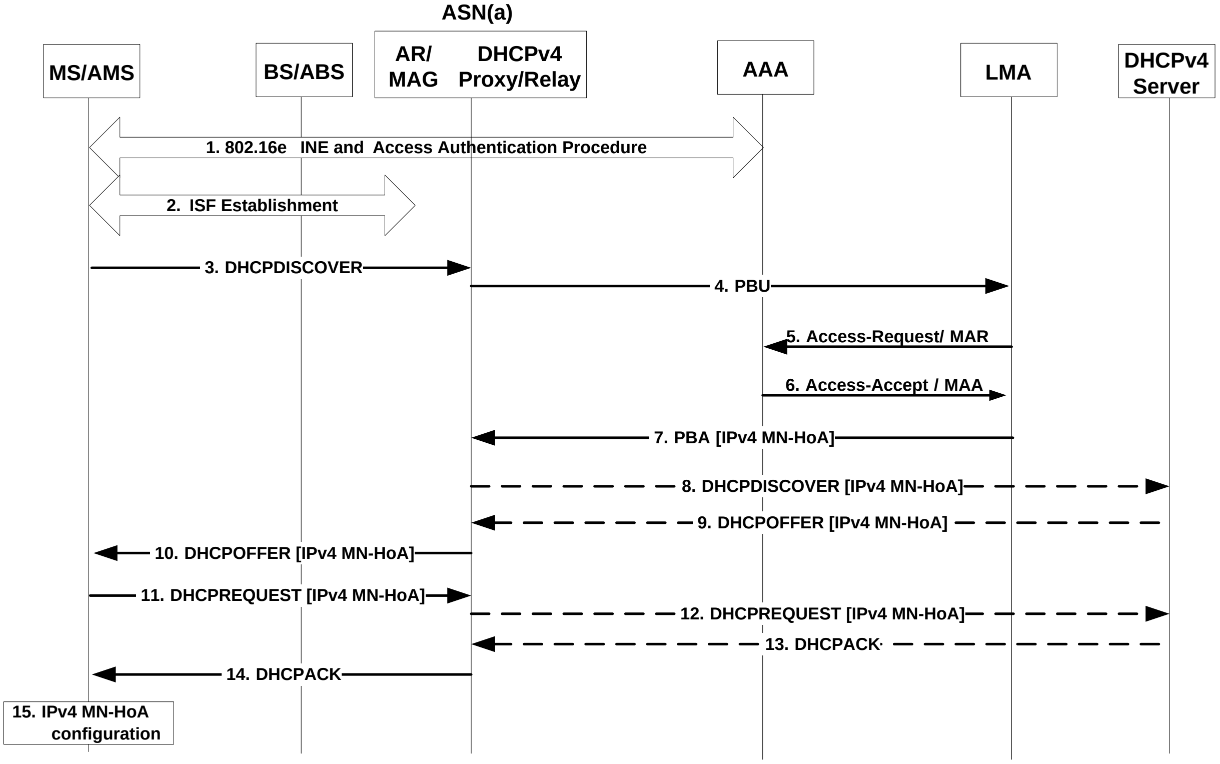

ASN(a)
MS/AMS
BS/ABS
AR/ MAG
DHCPv4 Proxy/Relay
AAA
LMA
DHCPv4 Server
1. 802.16e INE and Access Authentication Procedure
2. ISF Establishment
3. DHCPDISCOVER
4. PBU
5. Access-Request/ MAR
6. Access-Accept / MAA
7. PBA [IPv4 MN-HoA]
8. DHCPDISCOVER [IPv4 MN-HoA]
9. DHCPOFFER [IPv4 MN-HoA]
10. DHCPOFFER [IPv4 MN-HoA]
11. DHCPREQUEST [IPv4 MN-HoA]
12. DHCPREQUEST [IPv4 MN-HoA]
13. DHCPACK
14. DHCPACK
15. IPv4 MN-HoA configuration

Figure 4-155 - PMIP6 Connection Setup for an IPv4 MS/AMS

STEP 1

MS/AMS 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).

After successful WiMAX authentication and registration, the SFA ASN(a) initiates ISF establishment.

STEP 2

MS/AMS sends DHCPDISCOVER message in attempt to configure the IPv4 address on its network interface.

STEP 3

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/AMS. If IPv4 MN-HoA was provided in the MS/AMS 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 4–6

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/AMS 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/AMS MAY initiate request for an IPv6 HNP assignment if such service is authorized and supported by the network.

4.8.5.3.7.4 Connection setup using FIAA

Figure 4-156 presents PMIP6 connection setup procedure through FIAA-based address configuration. The same call flow can be used for configuring an IPv4 address and/or IPv6 prefix.

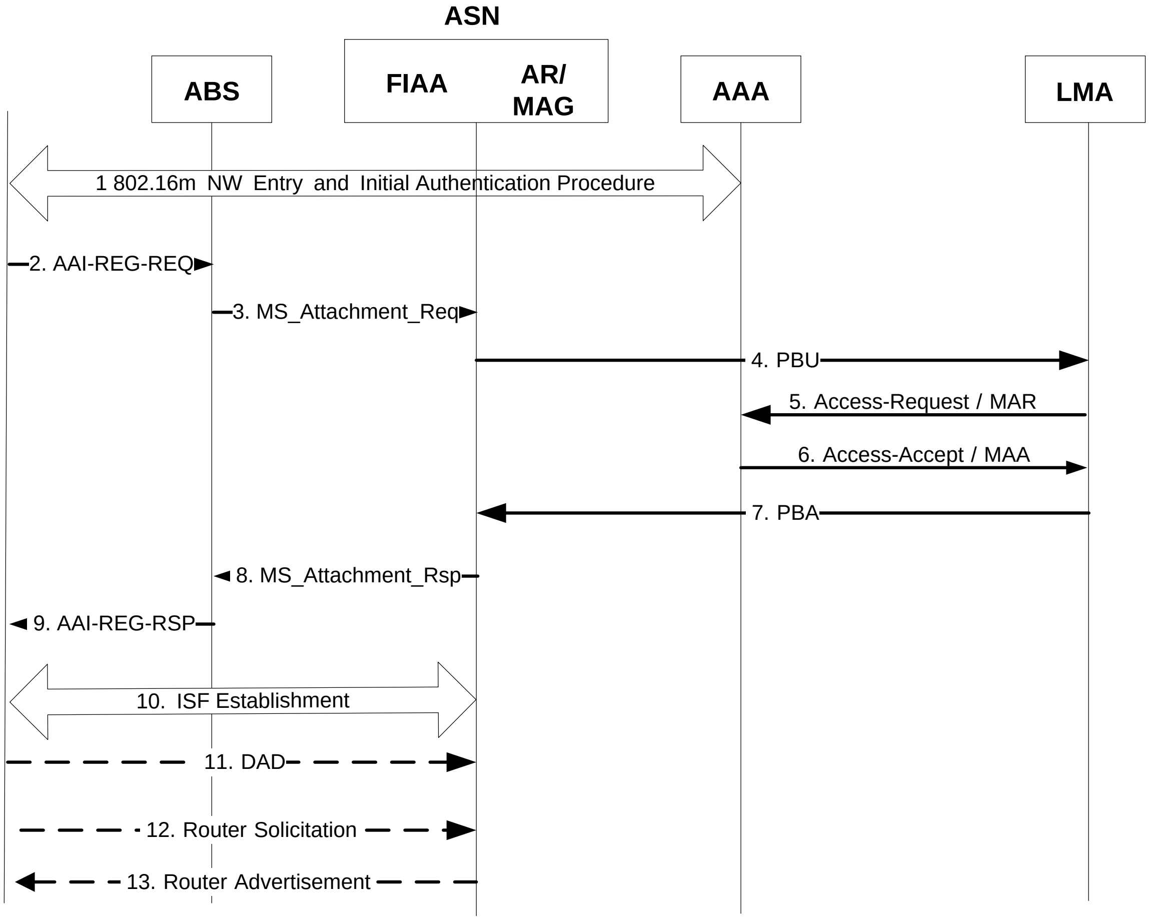


Figure 4-156 - PMIP6 Connection Setup using FIAA

STEP 1

AMS performs 802.16m 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 IPv4 HoA and IPv6 HNP information.

STEP 2

AMS sends the AAI-REG-REQ to the ABS. This message includes Host-Configuration-Capability-Indicator set to 1, and optionally Requested-Host-Configurations IE if there are additional options requested by the AMS.

STEP 3

ABS generates a MS_Attachment_Req by including the FIAA IEs received from the AMS.

STEP 4

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-HNP-PMIP6 option included in the PBU. If the IPv4 HoA was obtained from the HAAA, this information populates the Home-IPv4-HoA-PMIP6 option included in the PBU.

STEP 5

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 6

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 7

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 AMS's uplink and downlink payload forwarding. The PBA includes the AMS's assigned prefix in the HNP option, IPv4 address in Home IPv4 option, HO indicator value set to one, the ATT option set to value five, and the Link-local option populated as described in section 4.8.5.5.3.

STEP 8

Upon receiving the successful PBA, the ASN generates the MS_Attachment_Rsp. This message includes IPv6-Home_Network_Prefix IE whose payload is populated with the prefix info obtained from the PBA, IPv4-Host-Address IE whose payload is populated with the IPv4 address obtained from the PBA. Additional-Host-configurations IE may be included if there are additional options obtained from AAA (e.g., DNS server address).

STEP 9

ABS generates the AAI-REG-RSP by using the FIAA IEs received over MS_Attachment_Rsp.

STEP 10

ISF is established. If both an IPv6 prefix and IPv4 address are assigned then two ISFs are established.

STEP 11

Triggered by the establishment of the IPv6 ISF, the AMS configures a link local address, and global IPv6 address(es) using the prefix(es) it received in AAI-REG-RSP. AMS MAY start a duplicate address detection process to verify these addresses.

STEP 12

AMS MAY send a Router Solicitation message in attempt to learn the available routers on the link.

STEP 13

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). AMS ignores the RA Managed Flag setting as it has already configured its IP address using FIAA.

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/AMS and ASN SHALL support procedures for lease extension as per RFC 3315 [48].

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 FIAA Renewal

When FIAA is used, the allocated IP address is persistent throughout the WiMAX session. It does not have to be renewed. Therefore there are no requirements and procedures for renewing IP addresses with FIAA.

4.8.5.4.3 PMIP6 Lifetime Renewal

Session renewal in the case of PMIP6 service is about extending both the address lifetime of the MS/AMS and PMIP6 session lifetime of the LMA.

In case a stateless address autoconfiguration was used to configure the global address, the MS/AMS and ASN SHALL support mechanisms defined in [79] 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 sends 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 4-157 presents PMIP6 session renewal procedure by MAG ASN (a) triggering.

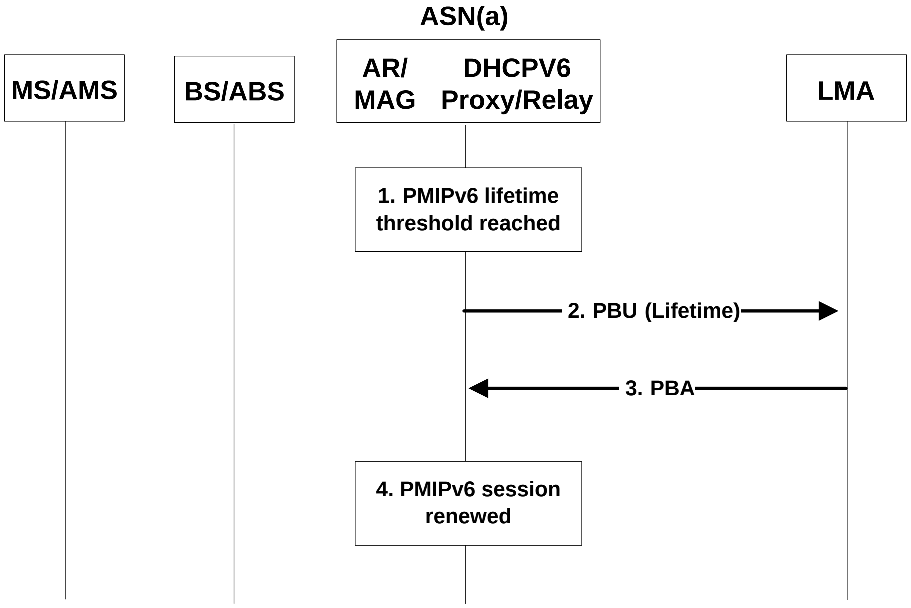


Figure 4-157 - PMIP6 Lifetime Renewal

STEP 1

The MAG in ASN (a) determines that the remaining lifetime of a particular PMIP6 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 PMIP6 session. The PBU includes Handoff Indicator option with the value set to 5 (HO state not changed), and the HNP assigned to the MS/AMS.

STEP 3

The LMA renews the lifetime of a particular PMIP6 session and MS/AMS'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/AMS's PMIP6 binding and the IP session.

4.8.5.5 PMIP6 CSN Anchored Mobility Handover

4.8.5.5.1 MS/AMS Requirements

There are no specific requirements towards the MS/AMS for the case of PMIP6 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/AMS after the HO, to hide the actual change of the attaching link.

When MS/AMS 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/AMS 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/AMS 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/AMS 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/AMS 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 4-119. 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 4-143.

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 4-144) message from the anchor Authenticator, it SHALL trigger PBU/PBA procedure to register MS/AMS'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/AMS, 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 4-120. Otherwise, it continues to anchor the DPF and acts as the AR/MAG for the MS/AMS.

The Target AR/MAG SHALL perform the PBU registration procedure following the guidelines specified in [82] (and [94] 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 5-57.

Upon receiving PBA from the LMA indicating registration success, the new AR/MAG in ASN(b) updates its local MS/AMS 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/AMS, 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 5.4.3.

LMA SHALL process and verify the contents of the PBU received from the target AR/MAG as defined in [82] (and [94] 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/AMS's binding cache entry with the new location information storing the new Proxy-CoA address. Upon successfully updating the MS/AMS'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). The LMA MAY send Revocation message to the previous AR/MAG to terminate binding (see 4.8.5.6).

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 5-57.

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/AMS mobility context.

4.8.5.5.6 FIAA Requirements

There are no requirements on FIAA for PMIP6 handovers.

4.8.5.5.7 PMIP6 CSN MM Flow(s)

Figure 4-158 presents the PMIP6 CSN Anchored mobility handover procedure for IPv6 and IPv4 MS/AMSs.

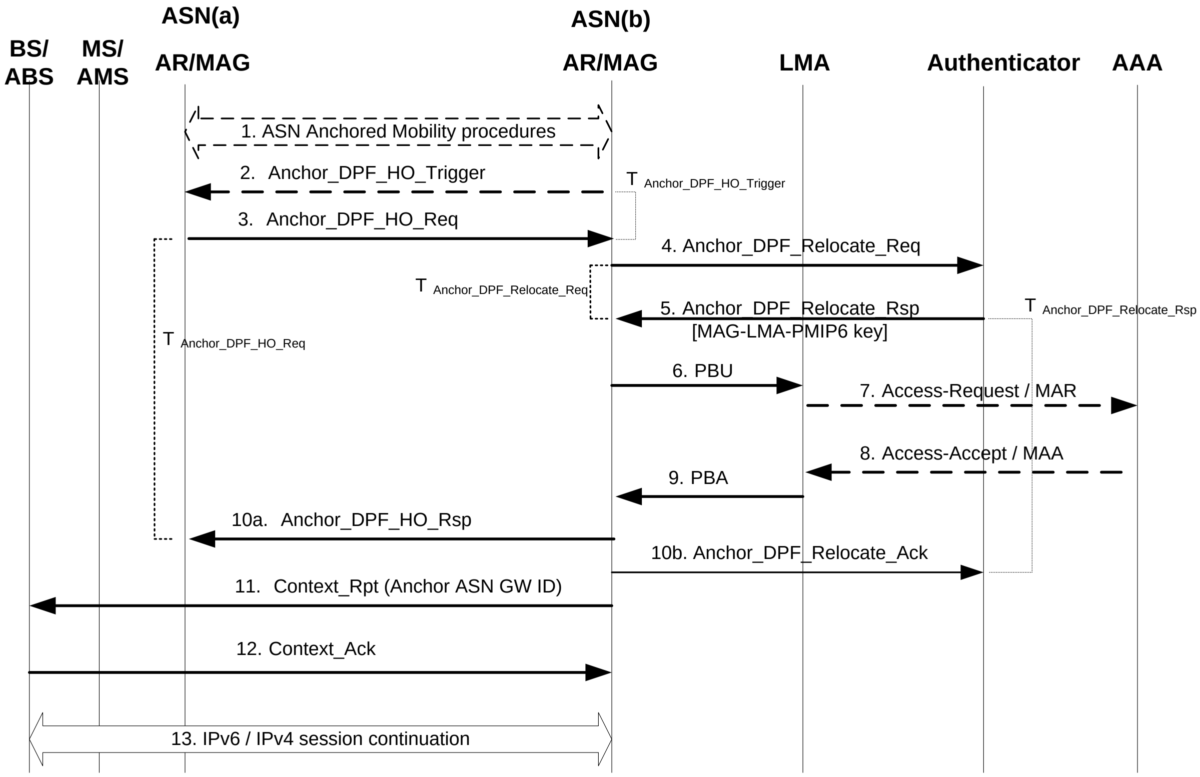

ASN(a)
ASN(b)
BS/ ABS
MS/ AMS
AR/MAG
AR/MAG
LMA
Authenticator
AAA
1. ASN Anchored Mobility procedures
2. Anchor_DPF_HO_Trigger
T Anchor_DPF_HO_Trigger
3. Anchor_DPF_HO_Req
4. Anchor_DPF_Relocate_Req
T Anchor_DPF_Relocate_Req
5. Anchor_DPF_Relocate_Rsp [MAG-LMA-PMIP6 key]
T Anchor_DPF_Relocate_Rsp
T Anchor_DPF_HO_Req
6. PBU
7. Access-Request / MAR
8. Access-Accept / MAA
9. PBA
10a. Anchor_DPF_HO_Rsp
10b. Anchor_DPF_Relocate_Ack
11. Context_Rpt (Anchor ASN GW ID)
12. Context_Ack
13. IPv6 / IPv4 session continuation

Figure 4-158 – PMIP6 CSN Anchored Mobility

STEP 1

MS/AMS 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 an 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 [72].

STEP 7

If required, the LMA sends an AAA request to the AAA server to authorize MS/AMS'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/AMS, 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 $T_{Anchor\_DPF\_HO\_Trigger}$ and releases the resources related with MS/AMS'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/ABS.

STEP 12

Upon receipt of the *Context_Rpt*, the BS/ABS updates the location of the Anchor DPF function for the attached MS/AMS 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 [82] (and [94] for IPv4 MS/AMS) for all subsequent IP packets exchanged with the MS/AMS, to achieve appearance of the same link attachment and thus uninterrupted IP session continuity for the MS/AMS.

Anchor_DPF_HO_Req message sent from the anchor ASN to the serving ASN for PMIP6 handover is defined as shown below in Table 4-142:

Table 4-142 – Anchor_DPF_HO_Req Message

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	
>Authenticator ID	5.3.2.19	M	

IE	Reference	M/O	Notes
>DHCP Relay Info	5.3.2.56	O	Information about the DHCP Relay. Anchor ASN SHALL include this TLV if 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.
>>>IPv6 Flow Label	5.3.2.470	O	
>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.

IE	Reference	M/O	Notes
>>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 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/AMS
>>> 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/AMS
>>> 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	

IE	Reference	M/O	Notes
>>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.
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/AMS 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 4-143 – 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/AMS.

IE	Reference	M/O	Notes
>>> Home Address (HoA)	5.3.2.77	O	IPv4 MN-HoA when operating PMIP6 mobility for an IPv4 MS/AMS.
>>> MAG IPv6 Address	5.3.2.415	M	IPv6 address of the target MAG, needed at the Authenticator for key derivation.

Table 4-144 – 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/AMS'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 4-145 – 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

4.8.5.5.8 Handover timers and timer considerations

This section provides the description of the timer used during PMIP6 CSN MM Handover.

- $T_{Anchor\_DPF\_HO\_Trigger}$: 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*.
- $T_{Anchor\_DPF\_HO\_Req}$: is started when serving ASN(a) sends an *Anchor_DPF_HO_Req* and is stopped upon receiving a corresponding *Anchor_DPF_HO_Rsp*.
- $T_{Anchor\_DPF\_Relocate\_Req}$: 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.
- $T_{Anchor\_DPF\_Relocate\_Rsp}$: 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 4-146 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-146 – Timer Values for PMIP6 CSN MM Handover Messages over R4/R3

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{Anchor\_DPF\_HO\_Trigger}$	TBD		TBD
$T_{Anchor\_DPF\_HO\_Req}$	TBD		TBD
$T_{Anchor\_DPF\_Relocate\_Req}$	TBD		TBD
$T_{Anchor\_DPF\_Relocate\_Rsp}$	TBD		TBD

4.8.5.5.9 Handover error conditions and recovery

This section describes error conditions associated with the PMIP6 CSN MM Handover procedure.

4.8.5.5.9.1 Timer Expiry

Table 4-147 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 4-147 Timer Max Retry Conditions.

Table 4-147 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{Anchor\_DPF\_HO\_Trigger}$	Target AR/MAG	PMIP6 CSN MM handover is aborted and further action of Serving/Target AR/MAG is implementation specific.
$T_{Anchor\_DPF\_HO\_Req}$	Serving AR/MAG	PMIP6 CSN MM handover is aborted and further action of Serving/Target AR/MAG is implementation specific.
$T_{Anchor\_DPF\_Relocate\_Req}$	Target AR/MAG	PMIP6 CSN MM handover is aborted and *Anchor_DPF_HO_Rsp* is sent to serving ASN(a) with Result Code set to Failure.
$T_{Anchor\_DPF\_Relocate\_Rsp}$	Anchor Authenticator	PMIP6 CSN MM handover is aborted.

4.8.5.5.9.2 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.

4.8.5.5.9.3 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.

4.8.5.5.9.4 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/AMS 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/AMS 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/AMS'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/AMS'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/AMS'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 FIAA Requirements

There is no explicit FIAA message for terminating the IP address configuration. Therefore, there are no requirements on FIAA function for PMIP6 Termination. Network exit procedure constitutes termination in this case.

4.8.5.6.6 PMIP6 Session Termination Flows

4.8.5.6.6.1 MS/AMS or MAG Session Termination

Figure 4-159 presents PMIP6 session termination procedure initiated by MS/AMS or the ASN-GW.

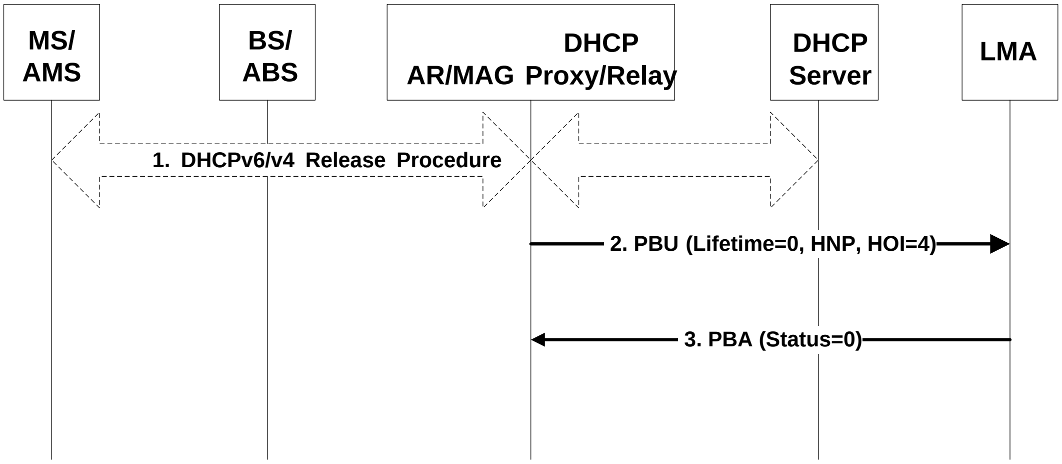


Figure 4-159 - PMIP6 Session Termination by MS/AMS / MAG

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/ABS even prior to step 1. The MS/AMS initiates the IP session release by performing DHCPv6 Release Procedure (DHCPv4 Release in case of an IPv4 MS/AMS) either self-initiated (MS/AMS triggered termination) or in response to the DREG directive received (ASN-GW triggered). For an IPv6 MS/AMS that was using stateless address autoconfiguration or FIAA there will not be a DHCPv6 release procedure. In such a case the MS/AMS has no means to inform the network it wants to terminate the IPv6 session, so the MS/AMS initiates the network exit procedure by sending *DREG_REQ* message with De-Registration Request Code=0x00 to the BS/ABS.

STEP 2

The AR/MAG discovers that the MS/AMS has performed L3 release or has detached from the network and sends a PBU to the associated LMA signaling MS/AMS detachment and binding de-registration. The PBU is constructed as specified in [82]; it has the Lifetime field value set to zero, must contain the HNP/IPv4-HoA assigned to that MS/AMS 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

4.8.5.6.6.2 AAA Session Termination

Figure 4-160 presents PMIP6 session termination procedure by the AAA.

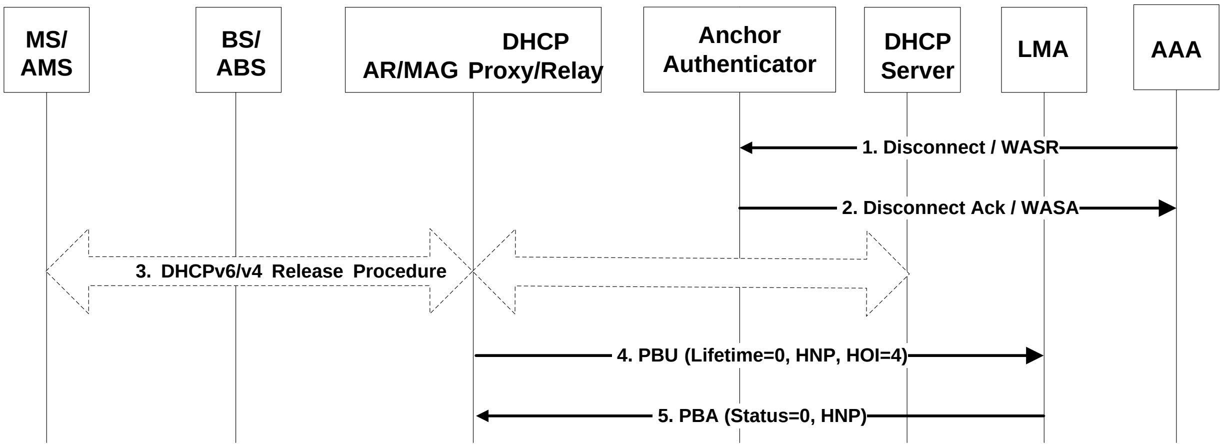


Figure 4-160 - PMIP6 Session Termination by AAA

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/AMS 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/AMS 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 or FIAA.

STEP 4

The AR/MAG discovers the MS/AMS release/detach and instigates PMIP6 binding release with the LMA as part of the MS/AMS 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/AMS's mobility binding is acknowledged with the appropriate PBU 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.

4.8.5.6.6.3 LMA Session Termination

Figure 4-161 presents PMIP6 session termination procedure by LMA.

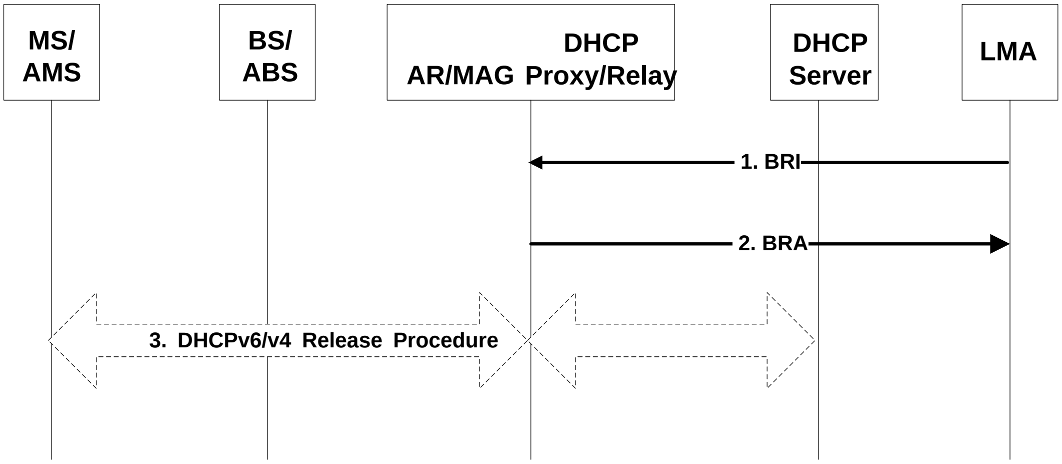


Figure 4-161 - PMIP6 Session Termination by LMA

STEP 1

If the MS/AMS'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/AMS 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 [96]. If the initial binding registration for the MS/AMS 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 5-58.

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/ABS. The MAG then releases the resources and forwarding rules associated with the MS/AMS 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 5-58). Only upon receiving the BRA (or retransmit timer expiry), the LMA releases the MS/AMS's proxy BCE and the associated forwarding tunnel.

STEP 3

If the IP address was configured through DHCP the MS/AMS performs the DHCPv6 Release Procedure (DHCPv4 Release in case of an IPv4 MS/AMS) in response to DREG directive received from the serving BS/ABS. The session termination gets completed following data path deregistration, NetExit and Accounting Stop procedures as specified in section 4.5.2.1.2.5

4.8.5.6.7 Handover timers and timer considerations

FFS

4.8.5.6.8 Handover error conditions and recovery

FFS

4.8.5.7 Dual Stack MS/AMS and PMIP6

This section only addresses DS MS/AMS and DS network related issues for PMIP6.

[Notes: In the scope of this section, DS MS/AMS means that the MS/AMS not only has the capability for both IPv4-CS and IPv6-CS but also is configured with both IPv4 address and IPv6 address.]

4.8.5.7.1 PMIP6 Security

Refer to section 4.8.5.1.

4.8.5.7.2 Management of IPv6 and IPv4 support

Refer to section 4.8.5.2.

4.8.5.7.3 PMIP6 Connection Setup Procedure for Dual Stack MS/AMS and Network

4.8.5.7.3.1 MS/AMS Requirements

The dual stack MS/AMS is not involved in PMIP6 mobility procedures and is only required to perform the common address acquisition and configuration procedure to obtain IP mobility management via PMIP6.

When MS/AMS has the capability for both IPv4-CS and IPv6-CS and is capable of acquiring and managing both IPv4 and IPv6 addresses independently(DS MS/AMS), it shall indicate that capability to BS/ABS in *REG-REQ* message. When receiving the both CS capability indication from BS/ABS in *REG-RSP* message, MS/AMS shall be commanded to acquire both IPv4 and IPv6 addresses. Once successfully completing the CS capability negotiation in *REG-REQ/RSP* interaction, MS/AMS shall expect two ISF pairs to be established, one pair is for IPv4-CS and the other pair is for IPv6-CS.

When FIAA is used, the IPv4 HoA and the IPv6 HNP are obtained by the AMS in REG-REQ/RSP procedure. When DHCP or stateless address autoconfiguration is used, MS/AMS shall initiate IP address acquisition for both service flows once both IPv4-CS and IPv6-CS based ISFs are established,

In the event that the ASN detects the MS/AMS loss the IP address for either the IPv4 ISF flow or IPv6 ISF flow and is unable to renew the IP address, then the ASN shall conduct the ISF loss behavior described in 4.6.4.2.

For IPv6 address configuration, DS MS/AMS SHALL act according to the information received from the AR/MAG in the (un)solicited Router Advertisement message when FIAA is not used. In that case, the address on MS/AMS'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 which the MS/AMS configures for itself is in PMIP6 terms referred to as MN-HoA.

For IPv4 address configuration, DS MS/AMS SHALL use either the DHCPv4 protocol or FIAA to configure the IP address (IPv4 MN-HoA) that is served with network-based PMIP6 mobility management.

When FIAA is used, dual stack AMS SHALL use it for both IPv4 and IPv6 configuration. Combining FIAA with DHCP or stateless address autoconfiguration for IP address configuration is prohibited.

Once successfully completing the negotiation with network for enabling both IPv4 and IPv6, Dual Stack MS/AMS shall configure IPv4 and IPv6 addresses separately and contemporaneously.

Once an IPv4 or IPv6 address is configured on DS MS/AMS, the MS/AMS can start data transfer on that IP version CS based service flow.

4.8.5.7.3.2 AR/MAG Requirements

The AR/MAG MUST obtain the Home Network Prefix and IPv4 Home Address before sending the first Router Advertisement or proceeding with DHCP message exchange. It means to allocate HNP and IPv4 MN-HoA including bootstrapping from the AAA server, or assignment by the LMA via PBU-PBA exchange.

The PMIP6 IP mobility management for the attaching MS/AMS is authorized on per-MS/AMS basis by the HAAA appending the appropriate authorization hint in the Access-Accept's PMIP6 Service Info attribute. Bit #1 and bit #2 are set if assignment and mobility of IPv6 address/prefix and IPv4 address are allowed. The AR/MAG SHALL act corresponding to the mobility type authorization when constructing the PBU message: if both mobility types are authorized, the PBU SHOULD include both HNP and IPv4 Home Address mobility options.For constructing the PBU and processing PBA response from the LMA, the AR/MAG SHALL follow requirements from [81] on MS/AMS attachment and initial binding registration, and receiving the PBA, with one key difference. Inline with PMIP6 service authorization results from the Access-Accept, the AR/MAG MUST apply in-band protocol security to the PBU sent to the LMA. When lower-layer transport security is only requested by the HCSN, AR/MAG will abandon explicit protection of PMIP6 control plane.

The initial PBU SHALL be formed in accordance with guidelines in section 5.7, and needs to contain valid MN identifier information, HO indicator option with value set to attach over a new interface (HOI=1), the Access Technology Type (ATT) option with value set to 5 to indicate WIMAX access, the link-local address option, and the Timestamp mobility option. The HNP and IPv4 HoA mobility options will be populated in the PBU if the information was obtained prior from the AAA server. The remaining PBU fields and mobility options are composed as defined in Table 5-57.

When IPv4 support in PMIP6 is utilized, the AR/MAG SHALL operate as specified in [81]. If the R3/R5 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 PBU at any time after successful access authentication and registration procedure. When multiple IP services are authorized specification of decision and trigger mechanisms that invoke AR/MAG to send PBU 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/AMS's PMIP6 session. When DHCPv6 configuration mode is authorized (i.e., when appropriate DHCP attribute(s) is(are) present in the Access-Accept, and FIAA is not used) 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/AMS corresponding to the address configuration mode associated with the MS/AMS's IP session; "A" flag is set in the Prefix Information Option if the MS/AMS 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/AMS 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.

4.8.5.7.3.3 LMA Requirements

The LMA SHALL support relevant PMIP6 AAA attributes defined in section 5.4.3 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 5-57.

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/AMS's BCE. At the time of the initial PBU, the LMA SHALL ensure that the MS/AMS is authorized for PMIPv6 mobility management.

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 IPv4 MN-HoA information, the LMA verifies that the MS/AMS is eligible for the allocated address e.g., against the AAA, and creates the BCE that binds the location of the MS/AMS with the MN ID and HNP/HoA it received. The LMA SHALL allow simultaneous registration of IPv4 MN-HoA and HNP for the MS/AMS when obtained from a single PBU message.

- In case AR/MAG does not include valid information option but the mobility option for HNP and/or IPv4 MN-HoA with ALL_ZERO value, the LMA MUST allocate HNP and/or IPv4 MN-HoA, assigns the information to the MS/AMS accordingly, and 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, but the details are outside the scope of this specification.

- 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/AMS. If a GRE Key option [93] 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. Both bindings for IPv4 MN-HoA and HNP shall use the same GRE tunnel.

The LMA SHALL manage the AR/MAG link-local address (LLA) unless the LLA parameter is 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.

4.8.5.7.3.4 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.

- The NAS SHALL explicitly inform the AAA of the IP transport and mobility abilities in scope of PMIP6 by including the indications in the PMIP6 Service Info attribute: bit for lower-layer transport security is set (when such support is in place), mobility management for IPv4 and IPv6 hosts is indicated when supported by the ASN, and IPv4 backhaul support is indicated when present.

- When MS/AMS attaches through a visited network, the VCSN SHALL indicate its PMIP6 support, i.e., the LMA & DHCP capabilities, if those are available by adding the corresponding indications in the VCS Network Capability TLV and other related attributes as part of the Access-Request message.

- If the HAAA acknowledges PMIP6 as an authorized IP service, it SHALL deliver the related PMIP6 subscriber/service profile information in the AAA Access-Accept message sent to the ASN and VCSN. The profile MUST provide the following information:

- PMIP6 listed under Authorized IP Network or Visited Authorized Network Services.
- Address of the home- and/or visited LMA designated for that specific MS/AMS's IP session. When IPv4 transport is to be used over R3/R5, the IPv4 address of the home- or visited-LMA has to be present.
- If available at the HAAA, the IPv6 Home Network Prefix (HNP) or the IPv4 MN-HoA or both of them may be present in the HAAA response.
- When DHCP service for PMIP6 is authorized, information associated with the DHCP Proxy/Relay functions e.g., the DHCPv4/v6 server address, DHCP security parameters, etc.
- Authorization of host IP mobility type (IPv6 and IPv4 bits SHALL be set in responding to the PMIP6 Service Info attribute).
- Directive on PMIP6 signaling protection method to be applied (lower-layer or in-band protocol security bits in the PMIP6 Service Info attribute).
- Security bootstrapping parameters (PMIP6 root key and the associated SPI).

The NAS/Authenticator SHALL store the obtained information locally and keep it available to the corresponding PMIP6 mobility entities in the ASN (MAG, DHCP function, etc.) throughout the IP session lifetime.

4.8.5.7.3.5 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.

For PMIP6 with IPv4 support service assigned to the MS/AMS, 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/AMS'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/AMS 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/AMS as a hint for the DHCP Server.

4.8.5.7.3.6 FIAA Requirements

If the AMS decides to configure IP addresses using FIAA, it SHALL use the FIAA IEs with the registration procedure. In that case the ABS and a FIAA compliant ASN-GW SHALL use FIAA as well, and SHALL NOT use DHCP or stateless address autoconfiguration.

ABS SHALL forward the FIAA IEs between the AMS and the FIAA compliant ASN-GW without any modifications (i.e., as-is).

The FIAA function learns the AMS' addressing information (i.e., HNP and/or IPv4 MN-HoA) either from the NAS or the AR/MAG. The NAS SHALL provide the HNP/MN-HoA to the FIAA 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 through binding update procedure (see Section 4.8.5.3.7.4).

4.8.5.7.3.7 DHCPv4 and Stateful DHCPv6 connection setup for Dual Stack MS/AMS and Network

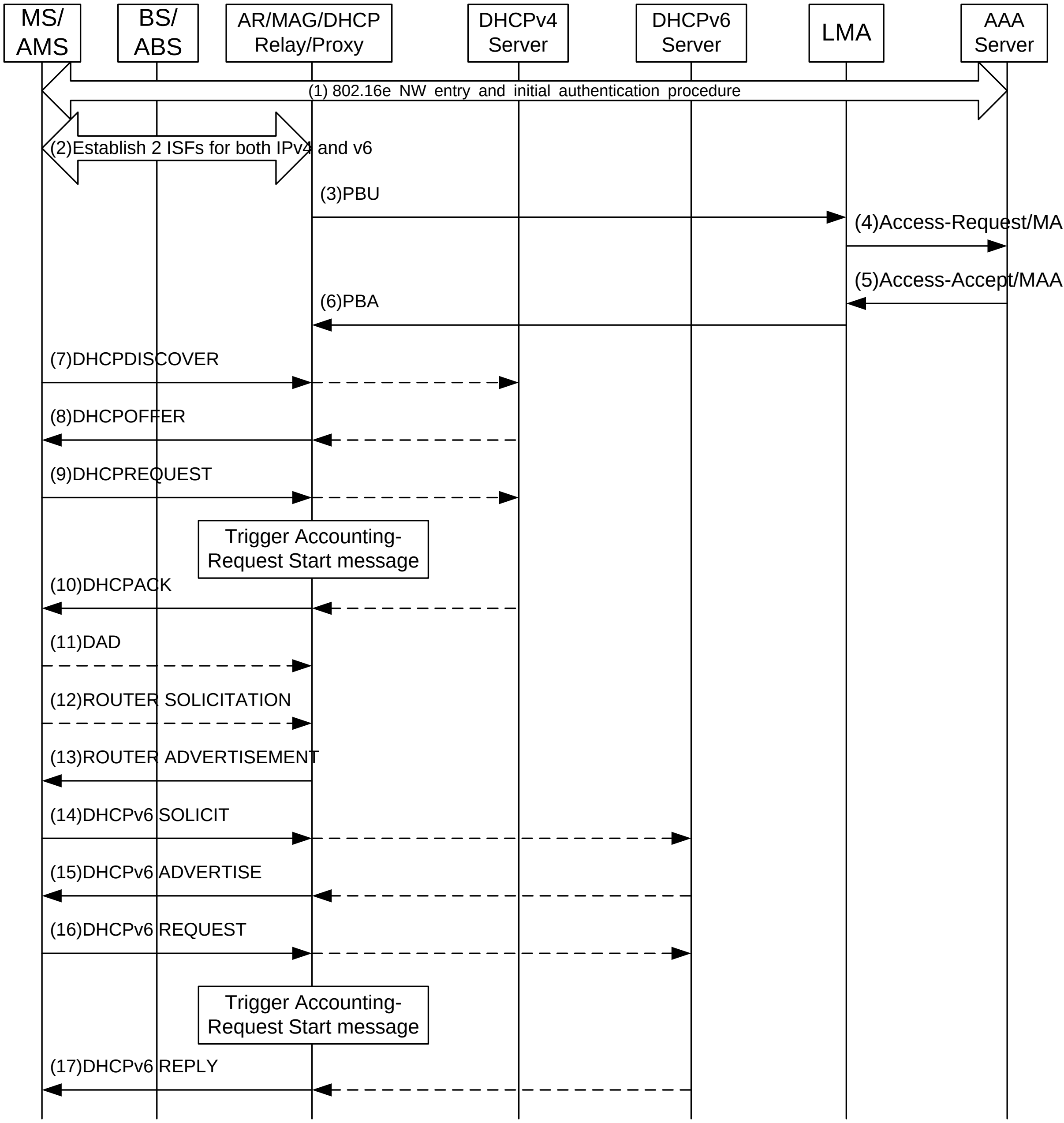


Figure 4-162 - DHCPv4 and Stateful DHCPv6 connection setup for Dual Stack MS/AMS and Network

STEP 1

MS/AMS 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 Home-IPv4-HoA-PMIP6, Home-HNP-PMIP6 and addresses of both the DHCPv4 server and the DHCPv6 server.

STEP 2

Two ISFs are established for both IPv4 and IPv6.

STEP 3

The AR/MAG in ASN 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 IPv4-HoA and HNP were obtained from the HAAA, this information populates Home-IPv4-HoA-PMIP6 and Home-HNP-PMIP6 included in the PBU.

Note: Step 3 is independent from step 2 and may occur at any given time after the network authentication/authorization and registration procedure.

STEP 4

After receiving the PBU message (message composition in section 4.8.5.3.3), the LMA initiates Authorization of MAG ASN 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/AMS's PMIP6 session. LMA creates the tunnel(s) towards the AR/MAG ASN and sets the routing rule directing all packets destined to the IPv4-HoA and all packets destined to HNP via the established PMIP6 tunnel(s).

STEP 6

The LMA sends the PBA to the AR/MAG ASN to confirm the initial binding registration and invokes creation of the dynamic bi-directional PMIP6 tunnel(s) for MS/AMS's uplink and downlink payload forwarding. The PBA includes the MS/AMS's assigned IPv4-HoA and the 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 7-10

MS/AMS 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 on the path to/from the associated DHCPv4 Server.

Receipt of DHCP Request from the MS/AMS shall be used as the trigger for Accounting Client to generate *Accounting-Request Start* message.

Note: Steps 7-10 are independent from steps 11-17. Step 7 can start after step 2.

STEP 11

MS/AMS configures a link local address, and MAY start a duplicate address detection process to verify it.

STEP 12

MS/AMS MAY send a *Router Solicitation* message in attempt to learn the available routers on the link.

STEP 13

AR/MAG ASN 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. If managed flag is not set to 1, then the MS/AMS performs auto-configuration of IPv6 address as described in next section.

STEP 14

In the case that Managed Flag is set to 1 in the *Router Advertisement* message, MS/AMS 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 provides the DHCP Proxy based address configuration.

In case of a DHCPv6 Relay, the DHCPv6 Relay ASN forwards the DHCPv6 *Solicit* message to the assigned DHCPv6 server. The message must include the HNP associated with the MS/AMS as a hint to the server.

STEP 15

In the DHCPv6 Proxy case, the DHCPv6 Proxy in ASN allocates the IPv6 HoA from the already known HNP and sends the DHCPv6 advertisement message to the MS/AMS.

In the case of a DHCPv6 Relay, the DHCPv6 Relay in ASN receives DHCPv6 *Advertisement* message from the DHCPv6 server and sends a DHCPv6 *response* message to the MS/AMS.

Note: Steps 11 to 14 can occur as soon as the ISF for IPv6 exists, i.e. Step 2; Steps 8 and 15 shall occur as soon as the MAG received the PBA, i.e. Step 6.

STEP 16

The MS/AMS sends a DHCPv6 Request message to ASN.

In case of a DHCPv6 Relay, the DHCPv6 Relay in ASN forwards the DHCPv6 *Request* message to the DHCPv6 server. The message includes the HNP associated with the MS/AMS as a hint to the server.

STEP 17

In the case of a DHCPv6 Proxy, the DHCPv6 Proxy in ASN responds to the MS/AMS’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 obtains the response from the server containing the assigned MN-HoA/128 and sends the DHCPv6 *response* message further to the MS/AMS.

Receipt of DHCPv6 *Request* from the MS/AMS shall be used as the trigger for Accounting Client to generate *Accounting-Request Start* message.

4.8.5.7.3.8 DHCPv4 and Stateless IPv6 address autoconfiguration connection setup for Dual Stack MS/AMS and Network

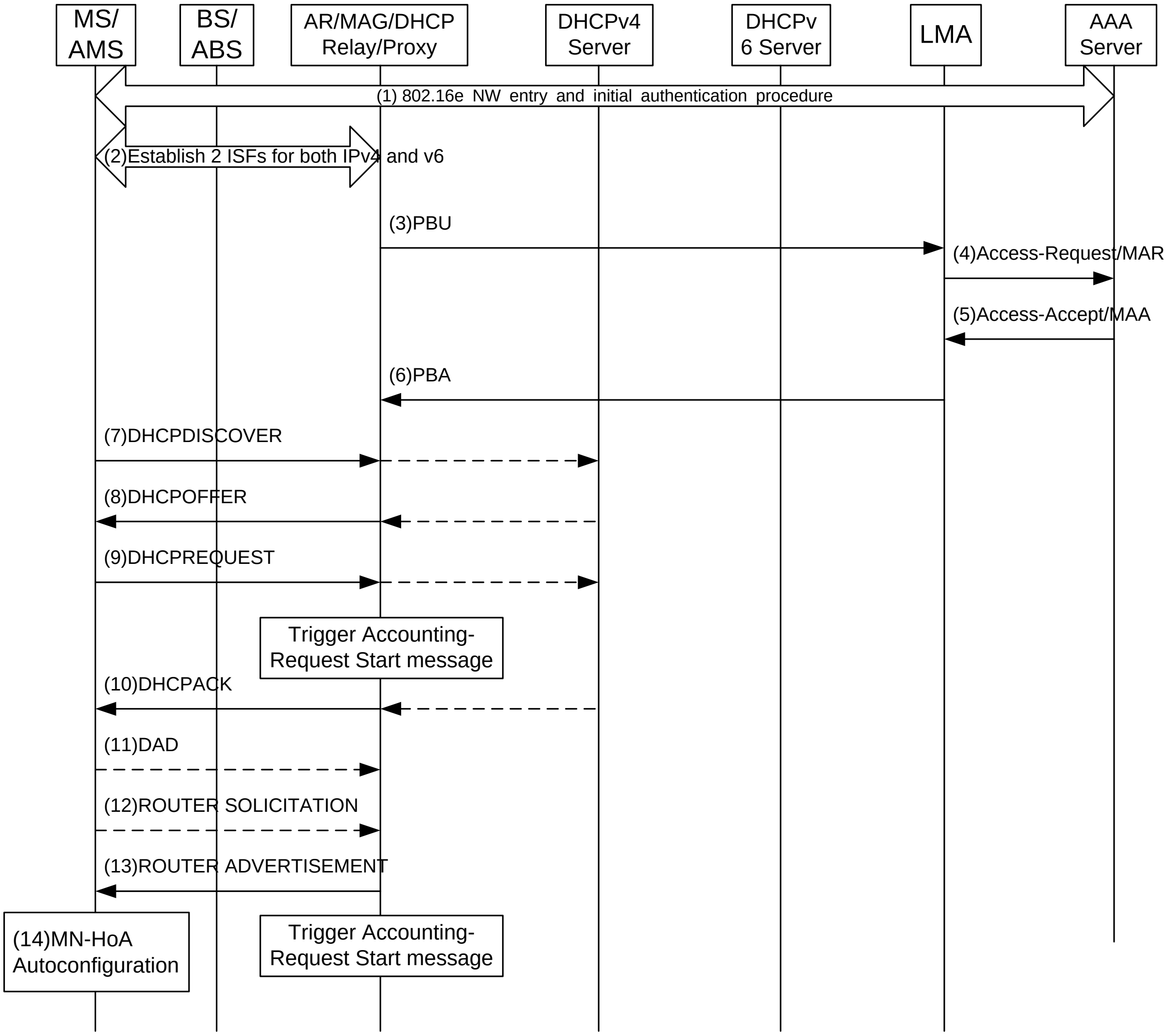


Figure 4-163 - DHCPv4 and Stateless address autoconfiguration connection setup for Dual Stack MS/AMS and Network

STEP 1

MS/AMS 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 Home-IPv4-HoA-PMIP6, Home-HNP-PMIP6.

STEP 2

Two ISFs are established for both IPv4 and IPv6.

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 IPv4-HoA and HNP were obtained from the HAAA, this information populates Home-IPv4-HoA-PMIP6 and Home-HNP-PMIP6 included in the PBU.

Note: Step 3 is independent from step 2 and may occur at any given time after the network authentication/authorization and registration procedure.

STEP 4

After receiving the PBU message (message composition in section 4.8.5.3.3), the LMA initiates Authorization of MAG ASN 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/AMS's PMIP6 session. LMA creates the tunnel(s) towards the AR/MAG ASN (a) and sets the routing rule directing all packets destined to the IPv4-HoA and all packets destined to HNP via the established PMIP6 tunnel(s).

STEP 6

The LMA sends the PBA to the AR/MAG ASN to confirm the initial binding registration and invokes creation of the dynamic bi-directional PMIP6 tunnel(s) for MS/AMS's uplink and downlink payload forwarding. The PBA includes the MS/AMS's assigned IPv4-HoA and the 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 7-10

MS/AMS 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 on the path to/from the associated DHCPv4 Server.

Receipt of *DHCP Request* from the MS/AMS shall be used as the trigger for Accounting Client to generate Accounting-Request Start message.

Note: Steps 7-10 are independent from steps 11-17. Step 7 can happen after step 2.

STEP 11

MS/AMS configures a link local address, and MAY start a duplicate address detection process to verify it.

STEP 12

MS/AMS MAY send a *Router Solicitation* message in attempt to learn the available routers on the link.

STEP 13

AR/MAG ASN sends the IPv6 *Router Advertisement* message with the HNP information enclosed in the Prefix information option which allows the MS/AMS to diretly autoconfigure its PMIP6 MN-HoA (the "A" flag SHALL be set to true, and Managed Flag MUST NOT be set to 1).

Transmission of the of *Router Advertisement* from the AR/MAG shall be used as the trigger for Accounting Client to generate *Accounting-Request Start* message.

Note: Steps 11 to 13 can occur as soon as the ISF for IPv6 exists, i.e. Step 2; Steps 8 shall occur as soon as the MAG received the PBA, i.e. Step 6.

STEP 14

The MS/AMS configures a globally routable IPv6 address using the stateless autoconfiguration process. The MS/AMS MAY trigger the duplicate address detection (DAD) for the IPv6 address which has been auto-configured on the network interface to verify its uniqueness on the link.

4.8.5.7.3.9 FIAA-based connection setup for dual stack AMS and network

See Section 4.8.5.3.7.4 for details.

4.8.5.7.4 PMIP6 Session Renewal Procedure

Refer to section 4.8.5.4.

4.8.5.7.5 PMIP6 CSN Anchored Mobility Handover

Refer to section 4.8.5.5.

4.8.5.7.6 PMIP6 Session Termination for Dual Stack MS/AMS and Network

4.8.5.7.6.1 One of the PMIP6 Session Termination for Dual Stack MS/AMS and Network

Not supported by this release. FFS.

4.8.5.7.6.2 Both of the PMIP6 Session Termination for Dual Stack MS/AMS and Network

The only difference between this section and section 4.8.5.6 is the interaction of PBU/PBA which shall include both of the IPv4 MN-HoA and HNP, other part shall refer to section 4.8.5.6.5.

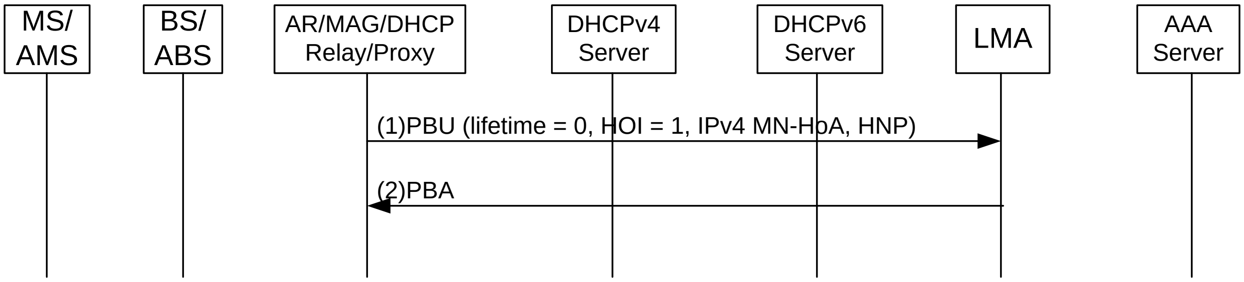


Figure 4-164 - General PBU/PBA for Dual Session Termination

STEP 1

The AR/MAG discovers the MS/AMS release/detach and initiates PMIP6 binding release with the LMA as part of the MS/AMS Network Exit procedure by sending the PBU with the Lifetime field set to value zero (also including corresponding MN-ID, HNP, IPv4 MN-HoA and HOI=4 information).

STEP 2

After successfully processing the De-registration PBU, the LMA releases the BCE and removes the forwarding tunnel(s) for the HNP, IPv4 MN-HoA. Removal of MS/AMS's mobility binding is acknowledged with the appropriate PBA sent back to the AR/MAG.

4.8.5.7.7 One PMIP6 Session Rebinding for Dual Stack MS/AMS and Network

Not supported by this release. FFS.

4.9 Radio Resource Management

4.9.1 Introduction

RRM is a function performed by the BS/ABS 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/ABS. See section 4.9.2 and Stage 2 Part 2 section 7.9 for details on RRM reference model.

Moreover, RRM may either work without R8 (i.e. based on R6 and R4), or by help of R8 being implemented between the BSs/ABSs 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/ABS 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/ABSs, 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.

The same RRM procedures are used for BS and ABS.

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/ABS controls its local RRA function and communicates with neighboring RRCs in other BS/ABSs. RRC-RRC communication may occur directly from BS/ABS to BS/ABS 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.

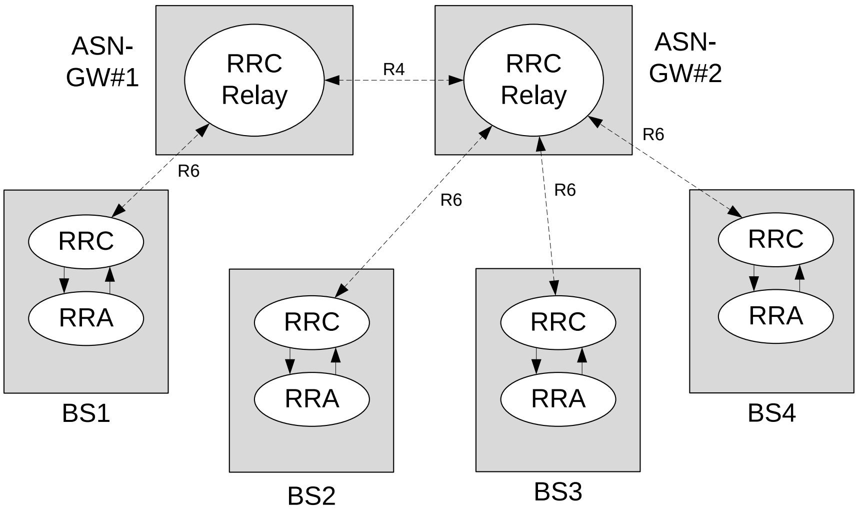


Figure 4-165 –RRC-RRC Communication on R6 and R4

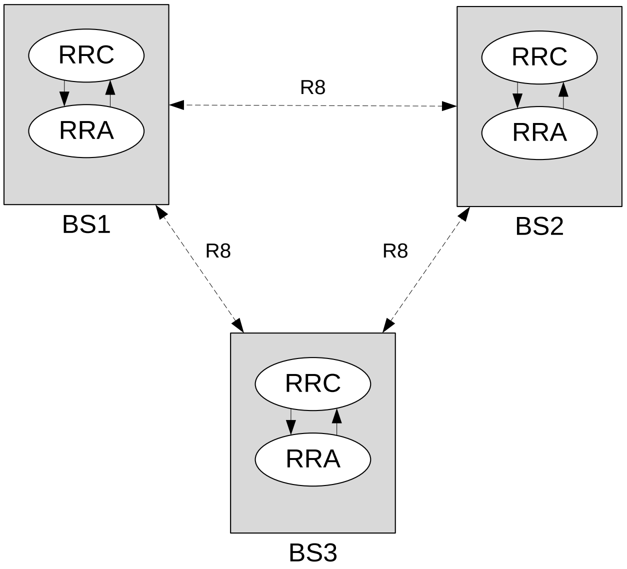


Figure 4-166 – RRC-RRC Communication on R8 (provided R8 is available)

The mapping of RRM primitives to R6 and R4, as well as R8 if any, is shown in Table 4-148.

Table 4-148 – RRM Procedures, Messages, Mapping to Reference Points

RRM Primitives	Communication Peers	Intra-ASN	Inter-ASN
Per-BS *Spare_Capacity_Req* and *Spare_Capacity_Rpt*	RRC – RRC	R4, R6, R8	R4
Per-BS *Radio_Config_Update_Req* and *Radio_Config_Update_Rpt* and *Radio_Config_Update_Ack*	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 4-165 "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/ABS Spare Capacity Reporting Procedure

4.9.3.1.1 Per-BS/ABS Spare Capacity Reporting Procedure with R6/R4

This procedure MAY be used by a BS/ABS (i.e., by the RRC in the BS/ABS) to retrieve information about the current load situation of any other BS/ABS, in particular of those neighboring Base Stations which MAY become candidate Target BSs/ABSs (TBSs) for Handover decisions.

Since the BS/ABS cannot communicate directly to neighboring BSs/ABSs, 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/ABS, or to another Relay RRC if the destination BS/ABS 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/ABSs.

Figure 4-167 shows the application of this procedure between two BSs/ABSs (Requesting BS/ABS and Reporting BS/ABS) with an ASN GW performing the Relay RRC function.

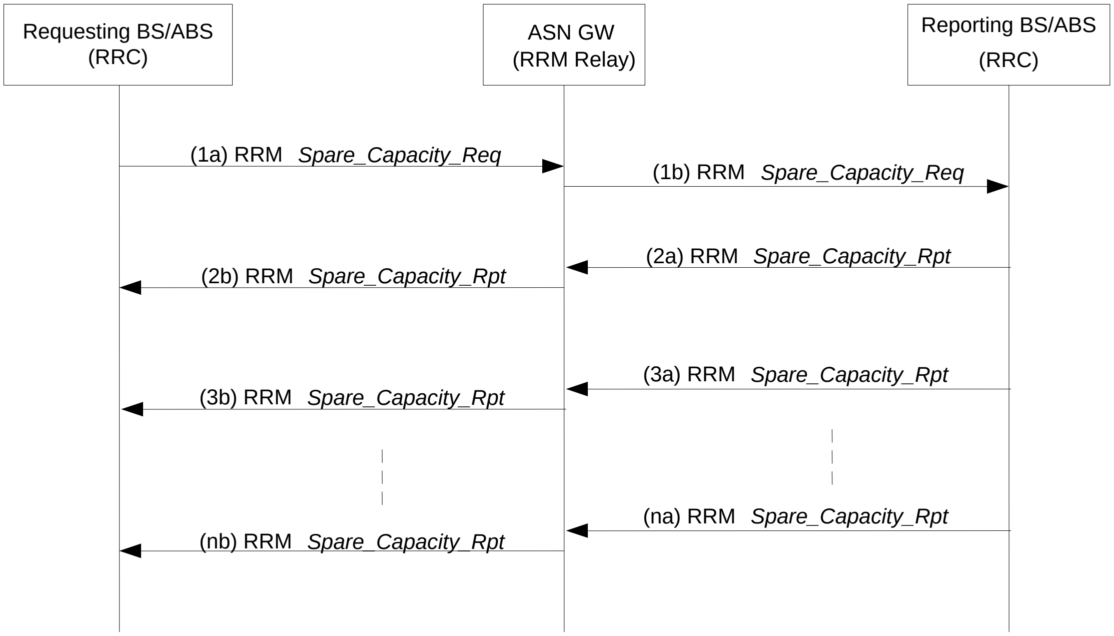

Requesting BS/ABS (RRC)
ASN GW (RRM Relay)
Reporting BS/ABS (RRC)
(1a) RRM Spare_Capacity_Req
(1b) RRM Spare_Capacity_Req
(2a) RRM Spare_Capacity_Rpt
(2b) RRM Spare_Capacity_Rpt
(3a) RRM Spare_Capacity_Rpt
(3b) RRM Spare_Capacity_Rpt
(na) RRM Spare_Capacity_Rpt
(nb) RRM Spare_Capacity_Rpt

Figure 4-167 – Per-BS/ABS Spare Capacity Reporting Procedure

STEP 1 (1a, 1b)

The "requesting BS/ABS" sends an RRM *Spare_Capacity_Req* to the ASN GW, requesting it to report about the available radio resources of a certain "Reporting BS/ABS"; 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/ABS. If that BS/ABS 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/ABS sends RRM *Spare_Capacity_Rpt* to ASN-GW, in direct response to the Request. ASN-GW relays that message to the Requesting BS/ABS.

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/ABS sends RRM *Spare_Capacity_Rpt* to ASN-GW, or subsequently in response to predefined events. ASN-GW relays that message to the Requesting BS/ABS.

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/ABS Spare Capacity Reporting Procedures with R8

In this case, the BS/ABS can communicate directly to neighboring BSs/ABSs via R8.

Figure 4-168 shows the application of this procedure between two BSs/ABSs (Requesting BS/ABS and Reporting BS/ABS) directly via R8.

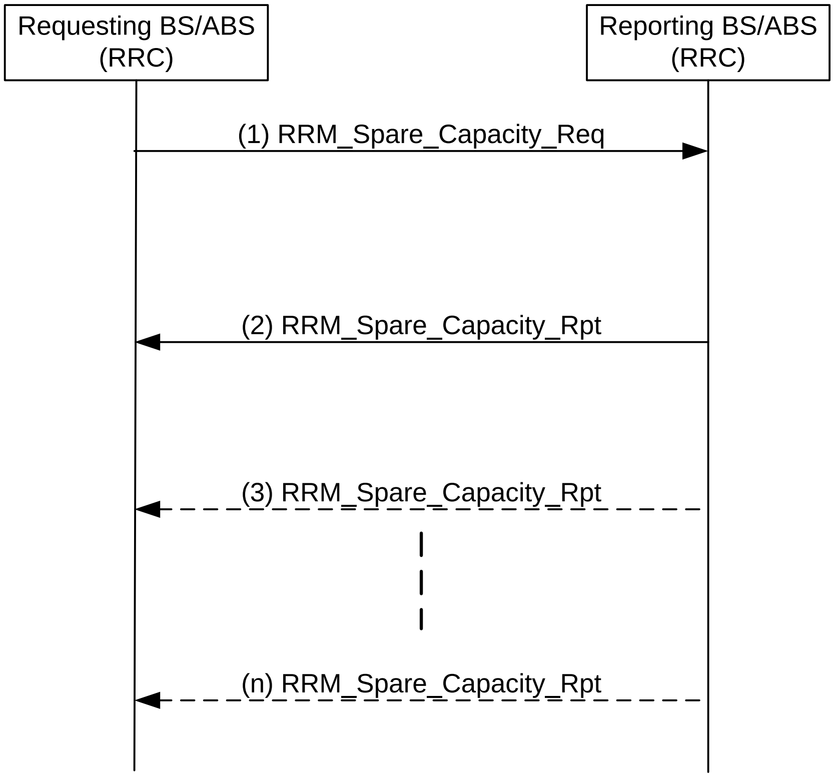

Requesting BS/ABS (RRC)
Reporting BS/ABS (RRC)
(1) RRM_Spare_Capacity_Req
(2) RRM_Spare_Capacity_Rpt
(3) RRM_Spare_Capacity_Rpt
(n) RRM_Spare_Capacity_Rpt

Figure 4-168 – Per-BS/ABS Spare Capacity Reporting Procedure via R8

STEP 1

The "requesting BS/ABS" sends an RRM Spare_Capacity_Req to the Reporting BS/ABS, requesting it to report about the available radio resources of the "Reporting BS/ABS"; reporting SHALL be done once, or periodically, or event driven.

The OP ID of this message is 0b001 ("Request/Initialization").

The Reporting BS/ABS sends RRM Spare_Capacity_Rpt to the Requesting BS/ABS, in direct response to the Request.

The OP ID of this message is 0b010 ("Response"). This ends the 2-way transaction.

, …, n

Optionally, the Reporting BS/ABS sends RRM Spare_Capacity_Rpt to the Requesting BS/ABS, 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/ABS Capacity Reporting Procedures

This section provides the message definitions for the R4, R6 and R8 messages in support of the Per-BS/ABS Spare Capacity Reporting Procedure. See also sections 5.2 and 5.3 for message and TLV definitions.

Table 4-149 – 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/ABS 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 *Spare_Capacity_Report* SHALL be sent only once by the reporting entity – TLV may be included based on local RRC policy. Decision to include this TLV is implementation specific. 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/ABS (RRA) as the measurement interval for producing the information requested by RRC. If omitted, the BS/ABS SHALL apply a default value.
RRM Reporting Period P	5.3.2.163	O	The Time P is used by BS/ABS (RRA) as the reporting period. If omitted, the BS/ABS SHALL apply a default value. When a report has been sent at time T, then the

IE	Reference	M/O	Notes
			next report SHALL be sent at T + P, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.
RRM Absolute Threshold Value J	5.3.2.157	O	The threshold value J is used by BS/ABS (RRA) as the absolute threshold for reporting.
RRM Relative Threshold RT	5.3.2.161	O	The threshold value RT is used by BS/ABS (RRA) to keep track of the threshold from the last measurement period.

1 **Table 4-150 – 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/ABS is out of service for the time being. Error Code 33 = BS/ABS 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/ABS 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/ABS policy. Decision to include this TLV is implementation specific.
>Radio Resource Fluctuation	5.3.2.142	O	Included based on local BS/ABS policy. Decision to include this TLV is implementation specific.
>DCD/UCD Configuration Change Count	5.3.2.48	O	Included based on local BS/ABS policy. Decision to include this TLV is implementation specific.

4.9.3.2 Per-BS/ABS Radio Configuration Update Procedure

4.9.3.2.1 Per-BS/ABS Radio Configuration Update Procedure with R6/R4

This procedure MAY be used by a BS/ABS to report some critical radio resource configuration update to the serving BS/ABS(RRC), such as DCD, UCD burst profile changes.

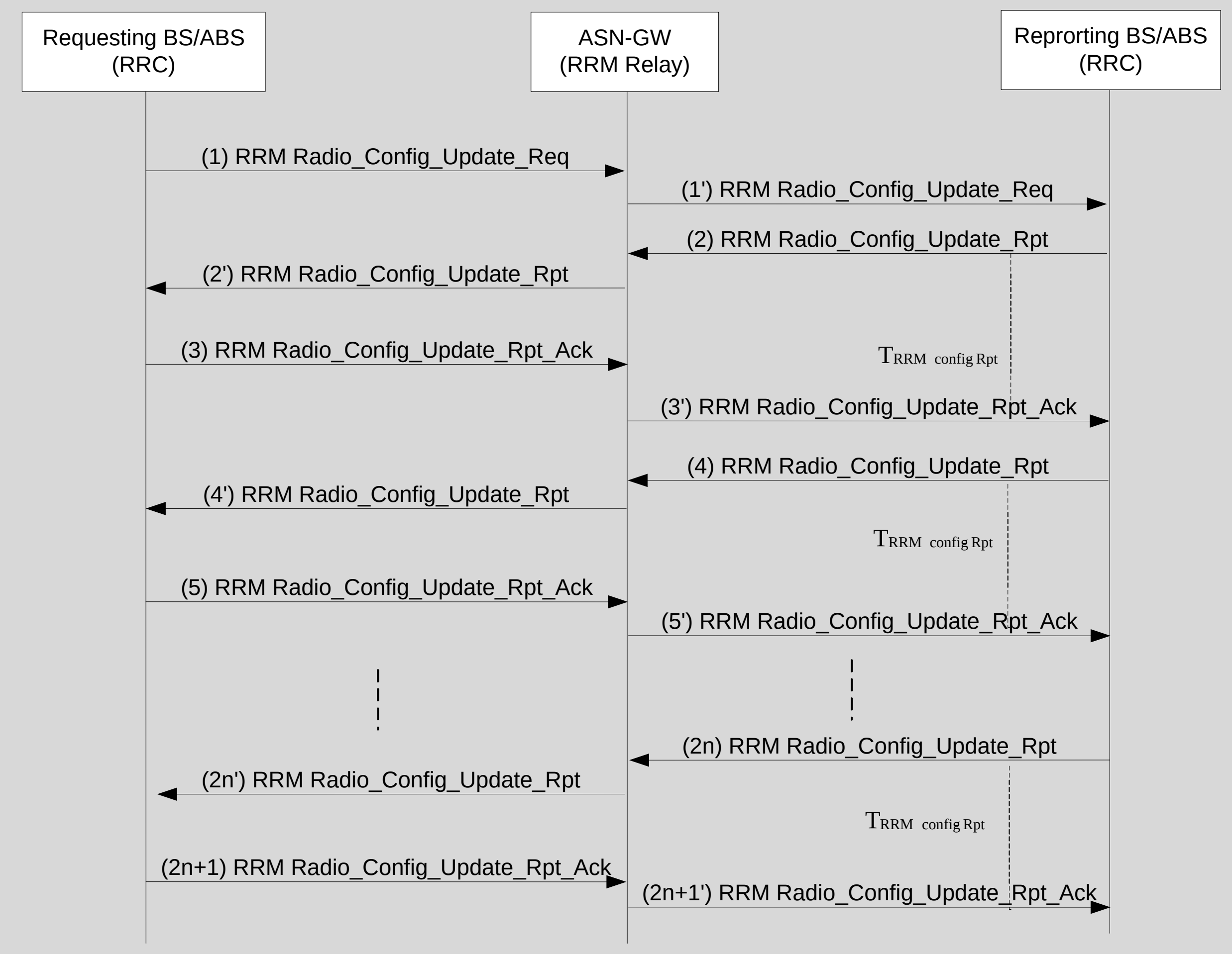

Requesting BS/ABS (RRC)
ASN-GW (RRM Relay)
Reprorting BS/ABS (RRC)
(1) RRM Radio_Config_Update_Req
(1') RRM Radio_Config_Update_Req
(2) RRM Radio_Config_Update_Rpt
(2') RRM Radio_Config_Update_Rpt
(3) RRM Radio_Config_Update_Rpt_Ack
TRRM config Rpt
(3') RRM Radio_Config_Update_Rpt_Ack
(4) RRM Radio_Config_Update_Rpt
(4') RRM Radio_Config_Update_Rpt
TRRM config Rpt
(5) RRM Radio_Config_Update_Rpt_Ack
(5') RRM Radio_Config_Update_Rpt_Ack
(2n) RRM Radio_Config_Update_Rpt
(2n') RRM Radio_Config_Update_Rpt
TRRM config Rpt
(2n+1) RRM Radio_Config_Update_Rpt_Ack
(2n+1') RRM Radio_Config_Update_Rpt_Ack

Figure 4-169 – Per-BS/ABS Radio Configuration Reporting Procedure

STEP 1 , 1'

The "requesting BS/ABS" 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/ABSs"; 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/ABSs. If a BS/ABS 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/ABS 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/ABS.

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/ABS 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/ABS. Once the Reporting BS/ABS 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/ABS 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/ABS.

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/ABS 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/ABS. Once the Reporting BS/ABS 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 ≥ 3)

Steps (2n and 2n’; n ≥ 3) are the same as Step 4.

STEP (2n+1, 2n+1’; n ≥ 3)

Steps (2n+1 and 2n+1’; n ≥ 3) are the same as Step 5. The 2-way transaction for report and ack may occur repeatedly until the Requesting BS/ABS 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*.

4.9.3.2.2 Per-BS/ABS Radio Configuration Update Procedure with R8

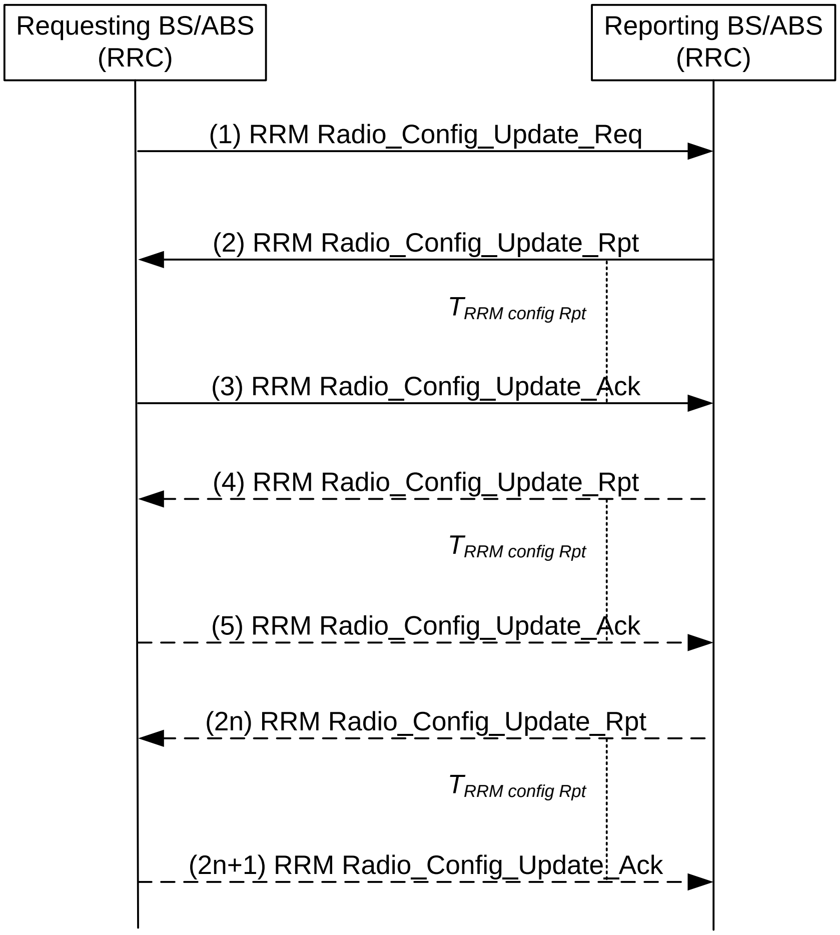

Requesting BS/ABS (RRC)
Reporting BS/ABS (RRC)
(1) RRM Radio_Config_Update_Req
(2) RRM Radio_Config_Update_Rpt
$T_{RRM\ config\ Rpt}$
(3) RRM Radio_Config_Update_Ack
(4) RRM Radio_Config_Update_Rpt
$T_{RRM\ config\ Rpt}$
(5) RRM Radio_Config_Update_Ack
(2n) RRM Radio_Config_Update_Rpt
$T_{RRM\ config\ Rpt}$
(2n+1) RRM Radio_Config_Update_Ack

Figure 4-170 – Per-BS/ABS Radio Configuration Update Reporting Procedure via R8

STEP 1

The "requesting BS/ABS" sends a "Radio configuration update-Request" via R8 to each "reporting BS/ABS", requesting it to report about the radio configuration parameters of the "Reporting BSs/ABSs"; 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.

STEP 2

The reporting BS/ABS sends "Radio Configuration update-Report" to the Requesting BS/ABS, 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").

STEP 3

The Requesting BS/ABS acknowledges receipt of Radio_Config_Update_Rpt by sending Radio_Config_Update_Ack via R8 to the Reporting BS/ABS. Once the Reporting BS/ABS 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/ABS sends an unsolicited "Radio Configuration update-Report" to the Requesting BS/ABS, as requested by the "RRM Reporting Characteristics", and starts timer TRRM-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/ABS acknowledges receipt of Radio_Config_Update_Rpt by sending Radio_Config_Update_Ack via R8 to the Reporting BS/ABS. Once the Reporting BS/ABS 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 2-way transaction.

STEP (2n; n ≥ 3)

Steps (2n; n ≥ 3) are the same as Step 4.

STEP (2n+1; n ≥ 3)

Steps (2n+1; n ≥ 3) are the same as Step 5. The 2-way transaction for report and ack may occur repeatedly until the Requesting BS/ABS 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/ABS Radio Configuration Update Procedure

This section provides the message definitions for the R4, R6 and R8 messages in support of the Per-BS/ABS Radio Configuration Update Procedure. See also section 5 for message and TLV definitions.

Table 4-151 – 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/ABSs 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 *Radio_Config_Update_Rpt* needs to be sent based on multiple events, then the corresponding bits have to be set to 1. If the optional reporting characteristics field is not specified, then the *Radio_Config_Update_Rpt* SHALL be sent only once. – This TLV is included based on local RRC policy. Decision to include this TLV is implementation specific. 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

IE	Reference	M/O	Notes
			and acknowledged with a similar value of zero (0000) in the corresponding RRM Spare capacity 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/ABS (RRA) as the reporting period. If omitted, the BS/ABS 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 4-152 – 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/ABS is out of service for the time being.
RRM Reporting Characteristics	5.3.2.162	O	Indicates the reason for this report. If the *Radio_Config_Update_Req* includes multiple events in the reporting characteristics, then the *Radio_Config_Update_Rpt* can include this attribute to indicate which event triggered the report by 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/ABS 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/ABS 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

IE	Reference	M/O	Notes
			configuration change count is presented. The DCD_settings is a TLV value that encapsulates the DCD message (excluding the generic MAC header and CRC) that the BS/ABS 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/ABS 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/ABS policy. Decision to include this TLV is implementation specific. TC SHALL be set to 1.
>HO Process Optimization/Reentry Process Optimization	5.3.2.78	O	Included based on local BS/ABS 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/ABS 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/ABS 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/ABS policy. Decision to include this TLV is implementation specific. TC SHALL be set to 1.
SA-Preamble Index	5.3.2.547	O	Indicate the SA-Preamble index of the carrier. This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.
A-Preamble Transmit Power		O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.
PHY Carrier Index	5.3.2.543	O	Physical carrier index of the ABS. This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.
S-SFH Change Count	5.3.2.546	O	S-SFH change count of the reference for the included SFH delta information. This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.
S-SFH setting	5.3.2.548	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.

1

Table 4-153 – 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 *Radio_Config_Update_Rpt* 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 4-178 employs one timer that is defined as follows:

- RRM configuration report timer ($T_{RRM\text{-}config\text{-}Rpt}$) – This timer is maintained by an RRC entity in an ASN to monitor the configuration update report. $T_{RRM\text{-}config\text{-}Rpt}$: 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 4-154 – RRM configuration report timer.

Timer	Entity	Reset(s)	Cause(s)	Action(s)
$T_{RRM\text{-}config\text{-}Rpt}$	ASN (RRC)	Receipt of Radio_Config_Update_Ack	Message gets lost due to congestion in the backhaul ASN overloaded, unable to process the Radio_Config_Update_Rpt message	When the timer expires, resend 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 4-155 shows the default value of timers and also indicates the range of the recommended timer values.

Table 4-155 – RRM-config-Rpt Timer Values

Timer	Default Value (ms)	Criteria	Maximum Timer Value (ms)
RRM-config-Rpt ($T_{RRM\text{-}config\_Rpt}$)	TBD	TBD	TBD

4.10 Paging and Idle-Mode MS/AMS 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/AMS SHALL perform the Location Update procedure when it meets the LU conditions as specified in the IEEE Std 802.16e/m specification. The MS/AMS 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/AMS and BS/ABS do not share a valid security context which means that BS/ABS is not able to receive a valid AK (e.g., MS/AMS crossed Mobility Domain boundaries or PMK has expired) or when the BS/ABS otherwise elects to direct the MS/AMS 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.

In case that the Location Update is for MS/AMS which entered idle mode in BS or LZone of ABS the MS/AMS is identified by its MSID. But, in case AMS entered idle mode in MZone of ABS, the AMS is identified by complete paging information(i.e. uniqueness of the AMS is achieved by the combination of the assigned Paging Group ID+ Paging Cycle,+Paging Offset + Deregistration ID).

4.10.2.1 Successful Secure Location Update - No Paging Controller Relocation

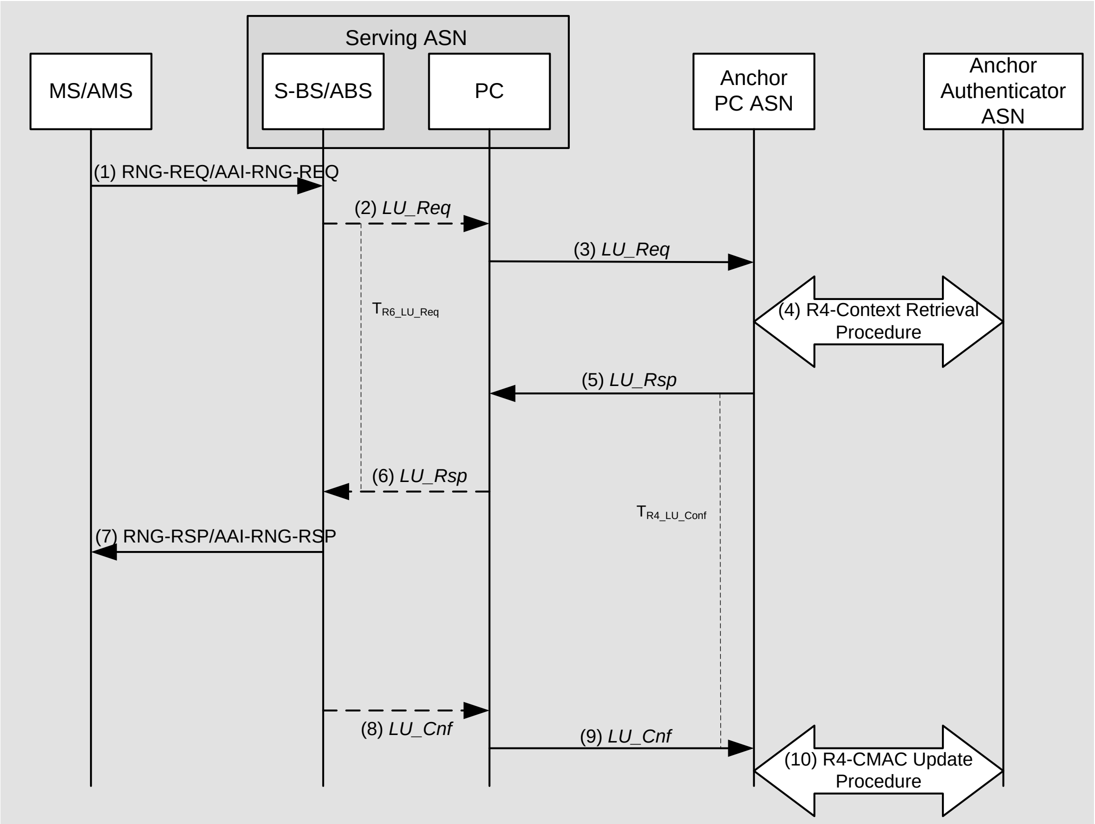


Figure 4-171 describes a MS/AMS initiated successful location update procedure with no Paging Controller relocation.

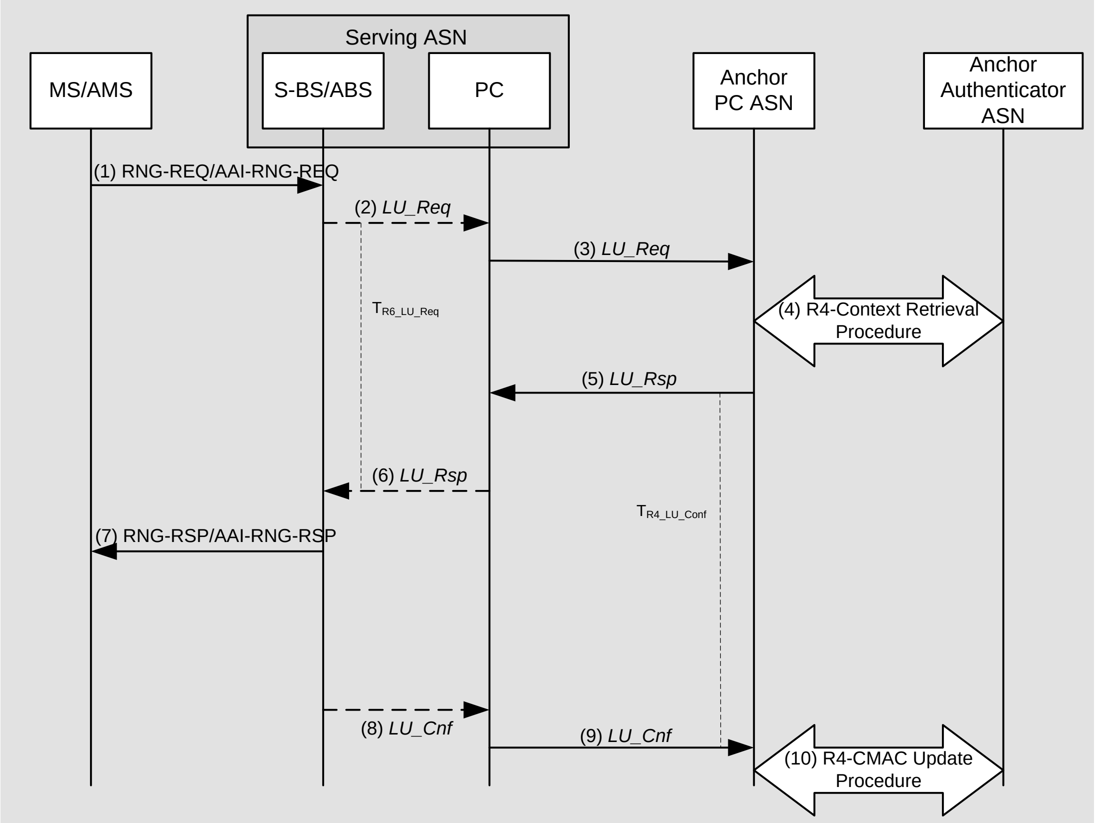


Figure 4-171 – Secure Location Update with no Paging Controller Relocation

STEP 1

The MS/AMS initiates a secure Location Update procedure when the conditions specified in the IEEE Std 802.16e/m specification are met. In BS or LZone of ABS, the MS/AMS 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/AMS, and the CMAC tuple.

In MZone of ABS, the AMS sends an AAI-RNG-REQ message, which includes the Ranging Purpose Indication set to indicate Idle Mode Location Update, the PC ID TLV, Deregistration ID, PGID, Paging Cycle, Paging Offset and the CMAC tuple.

STEP 2

The serving BS/ABS sends an R6 *LU_Req* message to the serving ASN-GW and starts timer $T_{R6\_LU\_Req}$.

When AMS is in BS or LZone of ABS, the message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the serving BS/ABS proposes an update to these parameters.

When AMS is in MZone of ABS, the message SHALL include the PG ID, Paging Offset, Paging Cycle and Deregistration ID TLVs for identification of AMS.

STEP 3

The Serving ASN (associated with the serving BS/ABS and local PC) sends an R4 *LU_Req* message to the Anchor PC ASN.

When AMS is in BS or LZone of ABS, the message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the Serving ASN proposes an update to these parameters.

When AMS is in MZone of ABS, the message SHALL include the PG ID, Paging Offset, Paging Cycle and Deregistration ID TLVs for identification of AMS.

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/ABS ID belongs to the MS Reattachment Zone. Only if the Serving BS/ABS ID belongs to the MS Reattachment Zone, the Anchor PC proceeds with step 4, otherwise it proceeds with step 5 to direct the MS/AMS to do initial network entry.

STEP 4

Anchor PC ASN SHOULD retain context information for the MS/AMS including its Authenticator ID, and initiate a Context Request procedure with the Anchor Authenticator ASN. Refer to section 4.10.5.9 for the call flow. If the Anchor Authenticator ASN has valid key material for the MS/AMS, it returns AK context for the MS/AMS to the Anchor PC ASN.

STEP 5

Upon successful retrieval of the AK context, the Anchor PC ASN sends an R4 *LU_Rsp* message back to the Serving ASN and starts timer $T_{R4\_LU\_Conf}$.

When AMS is in BS or LZone of ABS, the message includes the MSID, BSID, Authenticator ID, assigned PGID, Paging Offset, Paging Cycle, Anchor PC ID TLVs, and AK Context.

When AMS is in MZone of ABS, the message includes BSID, Authenticator ID, assigned PGID, Paging Offset, Paging Cycle, Deregistration ID, Anchor PC ID TLVs, and AK Context.

STEP 6

Upon receipt of the R4 *LU_Rsp* message, the Serving ASN-GW sends an R6 *LU_Rsp* message to the S-BS/ABS. Upon receipt the R6 *LU Rsp* message, S-BS/ABS stops timer $T_{R6\_LU\_Req}$. The message includes the, AK Context TLVs, as well as the assigned Paging Information TLV if they were included in the corresponding R4 message.

STEP 7

Based on the AK and AK context received from the Anchor PC, the Serving BS/ABS (associated with Local PC/Relay PC) successfully authenticates the RNG-REQ/AAI-RNG-REQ message received from the MS/AMS and sends a RNG-RSP/AAI-RNG-REQ message with CMAC, Successful *LU_Rsp* indication and New Anchor PC ID as specified in the IEEE Std 802.16 specification, to the MS/AMS.

STEP 8

The Serving BS/ABS sends an R6 *LU_Cnf* message to the serving ASN-GW. It includes the CMAC_Key_Count/AK_COUNT in the R6 *LU_Cnf*.

STEP 9

The Serving ASN sends an R4 *LU_Cnf* message to the Anchor PC ASN. Upon receipt of the message, The Anchor PC ASN updates the LR with MS/AMS Idle Mode information and stops timer $T_{R4\_LU\_Conf.}$

STEP 10

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/AK_COUNT. Refer to section 4.13 for the call flow.

4.10.2.2 Successful Secure Location Update with PC Relocation

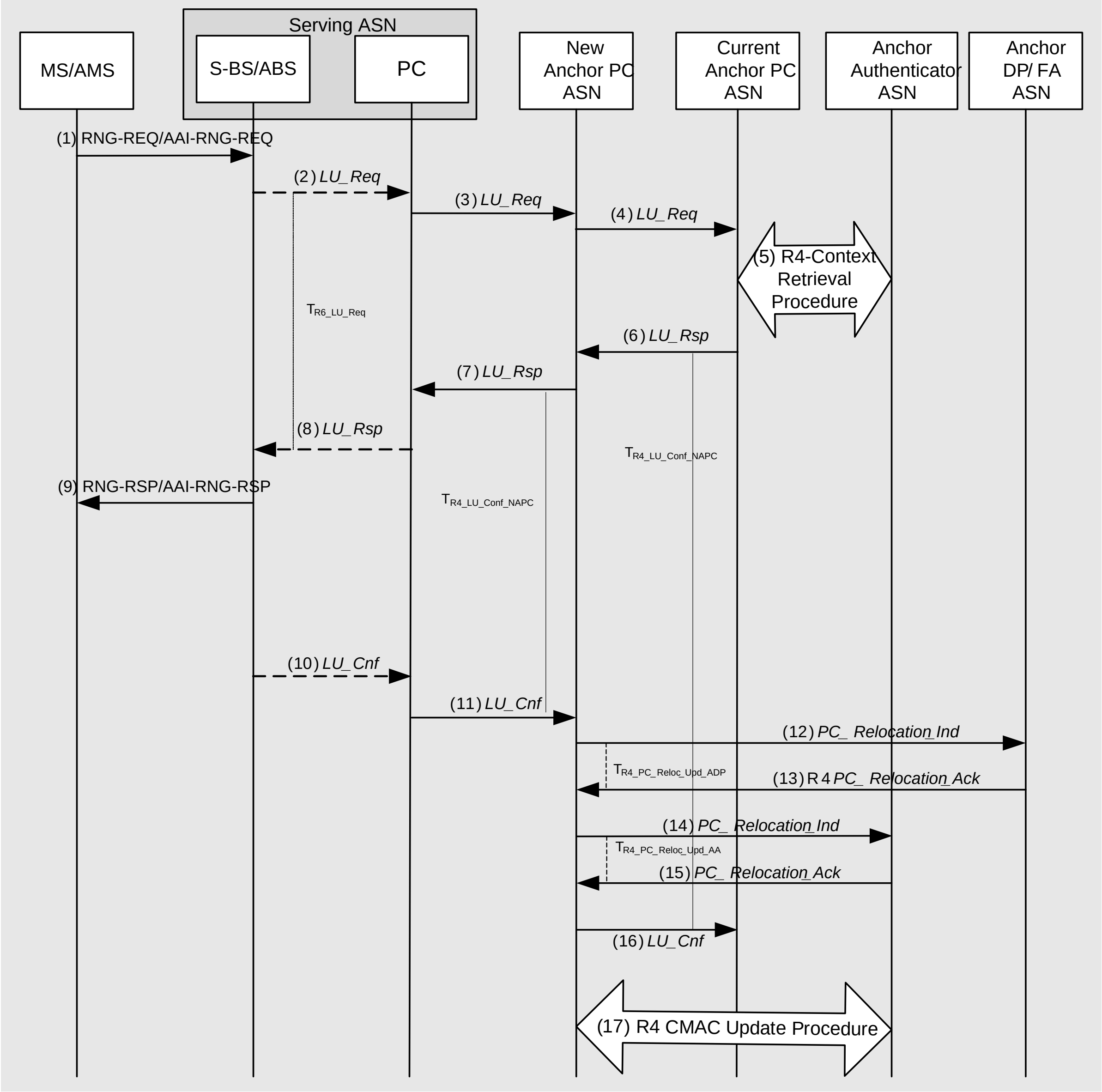


Figure 4-172 – Secure Location Update with Paging Controller Relocation

STEP 1

The MS/AMS initiates a secure Location Update procedure when the conditions specified in the IEEE Std 802.16e/m specification are met. The MS/AMS sends a RNG-REQ/AAI-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/AMS, and the CMAC tuple.

STEP 2

The serving BS/ABS sends an R6 *LU_Req* message to the serving ASN-GW and starts timer $T_{R6\_LU\_Req}$.

In case that the Location Update is for AMS which entered idle mode in MZone of ABS, in order of its anchor PC to recognize the AMS' identification the R6 *LU_Req* message SHALL include the current PG ID, the current Paging Offset, the current Paging Cycle and the current Deregistration ID TLVs (i.e. combination of the current PGID + the current Paging Offset + the current Paging Cycle + the current Deregistration ID determines uniquely the AMS).

The PC differntiates between location update form AMS in the MZone and MS/AMS in LZone by the presence of the MZone Indicator TLV. In case that the Location Update is for MS/AMS which entered idle mode in BS or LZone of ABS the MS/AMS is identified by MSID in the anchor PC.

The message may include the PG ID, Paging Offset, and Paging Cycle TLVs if the serving BS/ABS proposes an update to these parameters.

STEP 3

The Serving ASN (associated with the serving BS/ABS and local PC) sends an R4 *LU_Req* message to the Anchor PC ASN.

In case that the Location Update is for AMS which entered idle mode in MZone of ABS, in order of its anchor PC to recognize the AMS's identification the R4 *LU_Req* message SHALL include the current PG ID, the current Paging Offset, the current Paging Cycle and the current Deregistration ID TLVs. (i.e. combination of the current PGID + the current Paging Offset + the current Paging Cycle + the current Deregistration ID determines uniquely the AMS).

In case that the Location Update is for MS/AMS which entered idle mode in BS or LZone of ABS the MS/AMS is identified by MSID in the anchor PC.

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. For the AMS which entered idle mode in MZone of ABS when a relay PC ASN does not support Rel 2.0 functionality (i.e. the replay PC which does not support Rel2.0 functionality would find MSID field in the message header filled with 6byte long zeros), the relay PC ASN SHALL not initiate an anchor PC relocation.

If the MS mobility access classifier is fixed or nomadic, the Anchor PC checks whether the Serving BS/ABS ID belongs to the MS Reattachment Zone. Only if the Serving BS/ABS ID belongs to the MS Reattachment Zone, the Anchor PC proceeds with step 5, otherwise it proceeds with step 6 to direct the MS/AMS to do initial network entry.

STEP 5

Refer to section 4.10.5.9 for the call flow. If the Current Anchor PC ASN retains context information for the MS/AMS 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/AMS, it returns AK context for the MS/AMS 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 $T_{R4\_LU\_Conf}$.

In case of Location Update procedure for MS/AMS which entered idle mode in BS or LZone of ABS the message includes the MSID, BSID, Authenticator ID, assigned PGID, Paging Offset, Paging Cycle, Anchor PC ID TLVs, and AK Context.

In case of Location Update procedure for AMS which entered idle mode in MZone of ABS the message includes MSID, BSID, Authenticator ID, assigned PGID, Paging Offset, Paging Cycle, Deregistration ID, 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 candidate Anchor PC ASN doesn't request PC Relocation, the Current Anchor PC MAY still request to perform such procedure by including also the PC Relocation Indication TLV. If the candidate Anchor PC doesn't accept the relocation it will report Failure in step 6.

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. Specifically for AMS which entered idle mode in MZone of ABS the Paging information includes Deregistration ID), 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/ABS. 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/ABS (associated with Local PC/Relay PC) successfully authenticates the RNG_REQ message received from the MS/AMS and sends a RNG_RSP message with CMAC and Successful Location Update Response indication, as specified in the IEEE Std 802.16 specification, to the MS/AMS.

The Serving ABS (associated with Local PC/Relay PC) successfully authenticates the AAI-RNG-REQ message received from the AMS and send an AAI-RNG-RSP message, which is encrypted by AES-CCM per primary SA, with Successful Location Update Response indication, as specified in the IEEE802.16m specification, to the AMS.

STEP 10

The Serving BS/ABS 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/ABS). Alternatively the 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/AMS 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/AMS 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 $T_{R4\text{-}PC\_Reloc\_Upd\_AA.}$

STEP 15

The Anchor Authenticator ASN updates the Anchor PC for the MS/AMS 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 $T_{R4\text{-}PC\_Reloc\_Upd\_AA}$. At this point, New Anchor PC ASN hosts the Anchor PC function and becomes the 'new' Current Anchor PC ASN for the MS/AMS 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/AMS.

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 ASN. 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.
- $T_{R4\text{-}PC\_Reloc\_Upd\_AA:}$ 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/ABS upon transmission of an R6 *LU_Req* message from a Serving BS/ABS to a Serving ASN-GW. This timer is stopped upon reception of an R6 *LU_Rsp* message from the Serving ASN-GW.

Table 4-156 describes the default value and recommended range and duration for these timers.

Table 4-156 – 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

Timer	Default Values (msecs)	Criteria	Maximum Timer Value (msecs)
$T_{R6\_LU\_Req}$	TBD		TBD

4.10.2.4 Location Update Error Procedures

4.10.2.4.1 Timer MAX Retries

Table 4-157 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 4-157.

Table 4-157 – 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/AMS 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/AMS.
$T_{R4\_PC\_Reloc\_Upd\_AA}$	New Anchor PC ASN	New Anchor PC ASN notifies Relay Serving ASN of PC relocation. Serving ASN notifies MS/AMS.
$T_{R6\_LU\_Req}$	Serving BS/ABS	Serving BS/ABS notifies MS/AMS or Location Update failure.

4.10.2.4.2 Authenticator Context Retrieval failure

Whenever the RNG-REQ/AAI-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/AMS to begin the "Un-secure Location Update". Just as with failure of Secure Location Update, Unsecure Location Update is performed as MS/AMS network re-entry from Idle Mode process (see 4.10.2.4.4).

4.10.2.4.3 PC Relocation Failure

PC Relocation 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 candidate Anchor PC ASN is refused, then the candidate Anchor PC MAY force the MS/AMS 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/AMS receiving RNG-RSP/AAI-RNG-RSP message with "Failure of Idle Mode Location Update" should perform a network re-entry process (see 4.10). The network will re-authenticate the MS/AMS 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/AMS should not be changed.

If MS/AMS 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/AMS or network as described in section 5.3.2.373.

If MS/AMS 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/AMS or network should send DREG REQ/ AAI-DREG-REQ or DREG-CMD/AAI-DREG-RSP respectively 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/AMS 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/ABS ID belongs to the MS Reattachment Zone.

If the MS mobility access classifier is fixed or nomadic, the MS/AMS' Authenticator will reject AK context requests for the unauthorized BS/ABS based on Authenticator's knowledge of MS Reattachment Zone list. To reject the AK context request, the MS/AMS' Authenticator responds to Anchor PC with Context-Rpt message that includes appropriate Failure Indication value and excludes MS/AMS' AK context.

If the Serving BS/ABS 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/ABS sends RNG-RSP/AAI-RNG-RSP message back to MS/AMS setting Location Update Response TLV value as 0x01(Failure of Location Update) and directing the MS/AMS to do initial network entry.

4.10.2.5 Location Update Message Tables

Table 4-158 – LU_Req Primitive Structure

TLV	Description	M/O	Notes	Applicability
BS Info	5.3.2.26	M		1,2,3
> BS ID	5.3.2.25	M	BS ID indicating the BS/ABS where MS/AMS performs location update.	1,2,3
Paging Information	5.3.2.119	M	Paging Information TLV contains PAGING_CYCLE, PAGING OFFSET, PAGING_INTERVAL_LENGTH, Paging Group ID and Deregistration ID (DID). The BS/ABS may make a suggestion for Paging Cycle and Paging Offset for the MS/AMS performing LU.	1,2,3
> Paging Cycle	5.3.2.118	O	It is included if BS/ABS has a suggestion for this TLV.	1,2,3
> Paging Offset	5.3.2.120	O	It is included if BS/ABS has a suggestion for this TLV.	1,2,3
> Paging Interval Length	5.3.2.135	O	It is included if BS/ABS has a suggestion for this TLV. It is available only when MS/AMS entered idle mode in BS or	1,2

TLV	Description	M/O	Notes	Applicability
			LZone of ABS.	
> current Paging Cycle	5.3.2.481	M	Parameter which was assigned to AMS by anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> current Paging Offset	5.3.2.482	CM	Parameter which was assigned to AMS by anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> current Deregistration ID	5.3.2.483	CM	Deregistration ID assigned to AMS by anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
>current Paging Group ID	5.3.2.484	CM	Paging Group ID assigned to AMS by anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> Paging Group ID	5.3.2.123	O		1,2,3
>Anchor PC ID	5.3.2.12	M	"PC ID" field in DREG-REQ/AAI-DREG-REQ on R1 points to MS/AMS's anchor Paging Controller.	1,2,3
>Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS/AMS in Idle Mode, to be stored in Location Register during Location Update procedure.	1,2,3
>Anchor PC Relocation Destination	5.3.2.13	O	Identifier for destination Anchor PC in the event of Anchor PC relocation.	1,2,3
Network Exit Indicator	5.3.2.109	O	This is in case the LU is caused by Power Down Update.	1,2,3

1 **Table 4-159 – LU_Rsp Primitive Structure**

TLV	Reference	M/O	Notes	Applicability
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.	1,2,3
BS Info	5.3.2.26	M		1,2,3
> BS ID	5.3.2.25	M	BS ID indicating the BS/ABS where MS/AMS performs location update.	1,2,3
> AK Context	5.3.2.6	O	Security context required for BS/ABS to	1,2,3

TLV	Referenc e	M/O	Notes	Applicabi lity
			validate the received RNG-REQ/AAI-RNG-REQ message from MS/AMS and respond with RNG-RSP/AAI-RNG-RSP signed by a valid CMAC digest or encrypted by AES-CCM with a valid TEK, respectively.	
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
MS Info	5.3.2.103	O	MS Info to be included in the event of PC relocation.	1,2,3
>MSID	5.3.2.102	M	MSID SHALL be included for the case ONLY for AMS which entered idle mode in MZone of ABS.	3
>SBC context	5.3.2.174	CM	This TLV SHALL be included in R4 LU_Rsp in case of PC relocation.	1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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	1,2

TLV	Reference	M/O	Notes	Applicability
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>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.	1,2
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2,3
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>MAC Mode	5.3.2.322	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>Association type support	5.3.2.465	O		1,2
>>>Size of ICV	5.3.2.502	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	3
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC	1,2,3

TLV	Reference	M/O	Notes	Applicability
			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.	1,2
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2

TLV	Reference	M/O	Notes	Applicability
>>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.	1,2
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O		3
>>DEVICE_CLASS	5.3.2.504	O		3
>>CLC Request	5.3.2.505	O		3
>>Long TTI for DL	5.3.2.506	O		3
>>UL sounding	5.3.2.507	O		3
>>OL Region	5.3.2.508	O		3
>>DL resource metric for FFR	5.3.2.509	O		3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O		3
>>DL MIMO mode	5.3.2.512	O		3
>>feedback support for DL	5.3.2.513	O		3
>>Subband assignment A-MAP IE support	5.3.2.514	O		3
>>DL pilot pattern for MU MIMO	5.3.2.515	O		3
>>Number of Tx antenna of AMS	5.3.2.516	O		3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O		3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O		3
>>UL pilot pattern for MU MIMO	5.3.2.519	O		3
>>UL MIMO mode	5.3.2.520	O		3
>>Modulation scheme	5.3.2.521	O		3

TLV	Reference	M/O	Notes	Applicability
>>UL HARQ buffering capability	5.3.2.522	O		3
>>DL HARQ buffering capability	5.3.2.523	O		3
>>AMS DL processing capability per sub-frame	5.3.2.524	O		3
>>AMS UL processing capability per sub-frame	5.3.2.525	O		3
>>FFT size(2048/1024/512)	5.3.2.526	O		3
>>Authorization policy support	5.3.2.21	O		3
>>Inter-RAT Operation Mode	5.3.2.527	O		3
>>Supported Inter-RAT type	5.3.2.528	O		3
>>MIH Capability Supported	5.3.2.529	O		3
> REG context	5.3.2.144	O	This TLV SHALL be included in R4 LU_Rsp in case of PC relocation...	1,2,3
>>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.	1,2
>>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.	1,2
>>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. It is named as 'CS type support' in 16m.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ARQ is supported).	1,2
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2

TLV	Reference	M/O	Notes	Applicability
>>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.	1,2
>>>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.	1,2
>>>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.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. packing supported).	1,2
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ertPS supported).	1,2
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

TLV	Reference	M/O	Notes	Applicability
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O		3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O		3
>>Multicarrier capabilities	5.3.2.485	O		3
>>Zone Switch Mode Support	5.3.2.486	O		3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O		3
>>Interference mitigation supported	5.3.2.488	O		3
>>E-MBS capabilities	5.3.2.489	O		3
>>Channel BW and Cyclic prefix	5.3.2.490	O		3
>>frame configuration to support legacy R1.0	5.3.2.491	O		3
>>Persistent Allocation support	5.3.2.492	O		3
>>Group Resource Allocation support	5.3.2.493	O		3
>>Co-located coexistence capability support	5.3.2.494	O		3
>>HO Trigger Metric Support	5.3.2.326	O		3

TLV	Reference	M/O	Notes	Applicability
>>EBB Handover support	5.3.2.495	O		3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O		3
>>Capability for sounding antenna switching support	5.3.2.497	O		3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O		3
>>ROHC support	5.3.2.499	O		3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O		3
> Authenticator ID	5.3.2.19	CM	This TLV SHALL be included in R4 LU_Rsp in case of PC relocation.	1,2,3
>Anchor ASN GW ID	5.3.2.10	CM	This TLV SHALL be included in R4 LU_Rsp in case of PC relocation.	1,2,3
>SF Info	5.3.2.185	CM	This TLV SHALL be included in R4 LU_Rsp in case of PC relocation.	1,2,3
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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	1,2
>>CS Type	5.3.2.39	O	This TLV must be included in the transmitted message for the target ASN to setup flow.	1,2,3
>>ARQ Enable	5.3.2.345	CM	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e/m. This TLV SHALL be included if SF Info is included	1,2,3

TLV	Reference	M/O	Notes	Applicability
			in the transmitted message.	
>>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.	1,2,3
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1,2,3
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_SYNC_LOSS_TIMEOUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>SN Feedback Enabled field	5.3.2.468	O		1,2
>>FSN Size	5.3.2.469	O		1,2
>>>ARQ_SUB_BLOCK_SIZE	5.3.2.531	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_ERROR_DETECTION_TIMEOUT	5.3.2.534	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_FEEDBACK_POLL_RETRY_TIMEOUT	5.3.2.535	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>CID	5.3.2.29	O		1,2

TLV	Reference	M/O	Notes	Applicability
>>FID	5.3.2.471	O		3
>>SAID	5.3.2.169	O		1,2,3
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O		1,2,3
>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule.	1,2,3
>>> Classification Rule Priority	5.3.2.32	CM		1,2,3
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...	1,2,3
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.	1,2,3
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.	1,2,3
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.	1,2,3
>>>IPv6 Flow Label	5.3.2.470	O		1,2,3
>>QoS Parameters	5.3.2.141	CM	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
>>> DSCP	5.3.2.409	O	TC bit set to 1	1,2,3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1,2,3
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the	1,2,3

TLV	Reference	M/O	Notes	Applicability
			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.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3

TLV	Reference	M/O	Notes	Applicability
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1,2,3
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1,2,3
>>>Media Flow Type	5.3.2.94	O		1,2,3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1,2,3
>>>Reduced Resources Code	5.3.2.237	O		1,2,3
>>PHS Rule	5.3.2.127	O		1,2,3
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSF	0	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3

TLV	Reference	M/O	Notes	Applicability
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
> SA Descriptor (one or more)	5.3.2.170	O		1,2,3
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2

TLV	Referenc e	M/O	Notes	Applicabi lity
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>Mobility Access Classifier	5.3.2.423	O	Shall be included if the MS mobility Access classifier is fixed or nomadic..	1,2,3
>Reattachment Zone	5.3.2.424	O	Included if the MS mobility access classifier is included.	1,2,3
Paging Information	5.3.2.119	O	Paging Information TLV contains PAGING_CYCLE, PAGING OFFSET, PAGING_INTERVAL_LENGTH and Paging Group ID.	1,2,3
> current Paging Cycle	5.3.2.481	M	Parameter which was assigned to AMS by old anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> current Paging Offset	5.3.2.482	M	Parameter which was assigned to AMS by old anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> current Deregistration ID	5.3.2.483	M	Deregistration ID assigned to AMS by old anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
>current Paging Group ID	5.3.2.484	M	Paging Group ID assigned to AMS by old anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
>Paging Cycle	5.3.2.118	O	Anchor PC SHALL include this if BS/ABS had included a suggestion for this TLV.	1,2,3
>Paging Offset	5.3.2.120	O	Anchor PC SHALL include this if BS/ABS had included a suggestion for this TLV.	1,2,3
>Paging Interval Length	5.3.2.135	O	Anchor PC SHALL include this if BS/ABS had included a suggestion for this TLV. It is available only when MS/AMS entered idle mode in BS or LZone of ABS.	1,2,
> Deregistration ID	5.3.2.480	M	Deregistration IDassigned to AMS by a	3

TLV	Reference	M/O	Notes	Applicability
			new anchor PC. It SHALL be included to identify AMS when AMS entered idle mode in MZone of ABS. otherwise, it is not included.	
>Paging Group ID	5.3.2.123	O		1,2,3
> Old Anchor PC ID	5.3.2.113	O	This TLV is included in the event of PC relocation.	1,2,3
> Anchor PC ID	5.3.2.12	O	This TLV is included in the event of PC relocation.	1,2,3
>Anchor PC Relocation Request Response	5.3.2.14	O	"Accept" or "Refuse". Included only if PC Relocation is requested in R4 LU_Req	1,2,3
>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.	1,2,3
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.	1,2,3

1

2 **Table 4-160 – LU_Cnf Primitive Structure**

TLV	Description	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Location Update Failure code SHALL be included.	1,2,3
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	BS ID indicating the BS/ABS where MS/AMS performs location update.	1,2,3
> 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 *LU_Cnf*	1,2,3
MS Info	5.3.2.103	O		1,2,3
> CMAC_Key_ COUNT	5.3.2.34	M	Includes BS/ABS value of CMAC_KEY_COUNT to update an Authenticator's.	1,2,3
Paging Information	5.3.2.119	O	The BS/ABS SHALL reflect the Paging Cycle, Paging Offset, Paging Interval Length and Paging Group Id received in the LU_Rsp.	1,2,3
>Paging Cycle	5.3.2.118	O	Anchor PC SHALL include this if BS/ABS had included a suggestion for this	1,2,3

TLV	Description	M/O	Notes	Applicability
			TLV. It SHALL be included to identify AMS when AMS entered idle mode in MZone of ABS.	
>Paging Offset	5.3.2.120	O	Anchor PC SHALL include this if BS/ABS had included a suggestion for this TLV. It SHALL be included to identify AMS when AMS entered idle mode in MZone of ABS.	1,2,3
>Paging Interval Length	5.3.2.135	O	Anchor PC SHALL include this if BS/ABS had included a suggestion for this TLV. It is available only when MS/AMS entered idle mode in BS or LZone of ABS.	1,2
> Deregistration ID	5.3.2.480	M	Deregistration IDassigned to AMS by a new anchor PC. It SHALL be included to identify AMS when AMS entered idle mode in MZone of ABS. otherwise, it is not included.	3
>Paging Group ID	5.3.2.123	O	It SHALL be included to identify AMS when AMS entered idle mode in MZone of ABS.	1,2,3
>Anchor PC ID	5.3.2.12	O	Included if PC relocation was requested earlier.	1,2,3
>Relocation Success Indicator	5.3.2.149	O	Success if Relocation was accepted by destination and completed.	1,2,3

1 **Table 4-161 – Context_Req Primitive Structure**

TLV	Reference	M/O	Notes	Applicability
Context Purpose Indicator	5.3.2.36	M		1,2,3
BS Info	5.3.2.26	M	Serving BS/ABS.	1,2,3
>BS ID	5.3.2.25	M	The BSID received in the R4 LU.	1,2,3
Paging Information	5.3.2.119	O		1,2,3
>Anchor PC Relocation Destination	5.3.2.13	O	Identifier for destination Anchor PC, included in the event of Anchor PC relocation.	1,2,3

Table 4-162 – Context_Rpt Primitive Structure

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Provide failure indication for this message.	1,2,3
Context Purpose Indicator	5.3.2.36	M		1,2,3
BS Info	5.3.2.26	M	Serving BS/ABS.	1,2,3
>BS ID	5.3.2.25	M	BSID received in the corresponding R4 Context Request.	1,2,3
>AK Context	5.3.2.6	M		1,2,3
>>AK	5.3.2.5	M		1,2,3
>>AK ID	5.3.2.7	M		1,2,3
>>AK Lifetime	5.3.2.8	M		1,2,3
>>AK SN	5.3.2.9	M		1,2,3
>>CMAC_KEY_COUNT	5.3.2.34	M		1,2,3

Table 4-163 – PC_Relocation_Ind Primitive Structure

TLV	Reference	M/O	Notes	Applicability
Anchor PC ID	5.3.2.12	M	Indicating the new Anchor PC ID.	1,2,3
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.	1,2,3

Table 4-164 – PC_Relocation_Ack Primitive Structure

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3

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/AMS;
- Location update forced by the network for this MS/AMS;
- Network initiated MS/AMS network re-entry;
- Cancel *Paging_Announce* once the MS/AMS 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/AMS. 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/AMS, 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/AMS last performed a location update, and also neighboring BS/ABS topology to allow for multi-step paging. The Anchor PC directly sends R4 *Paging_Announce* messages to only the Relay PCs associated with the MS/AMSs current PGID (see Figure 4-173). 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.

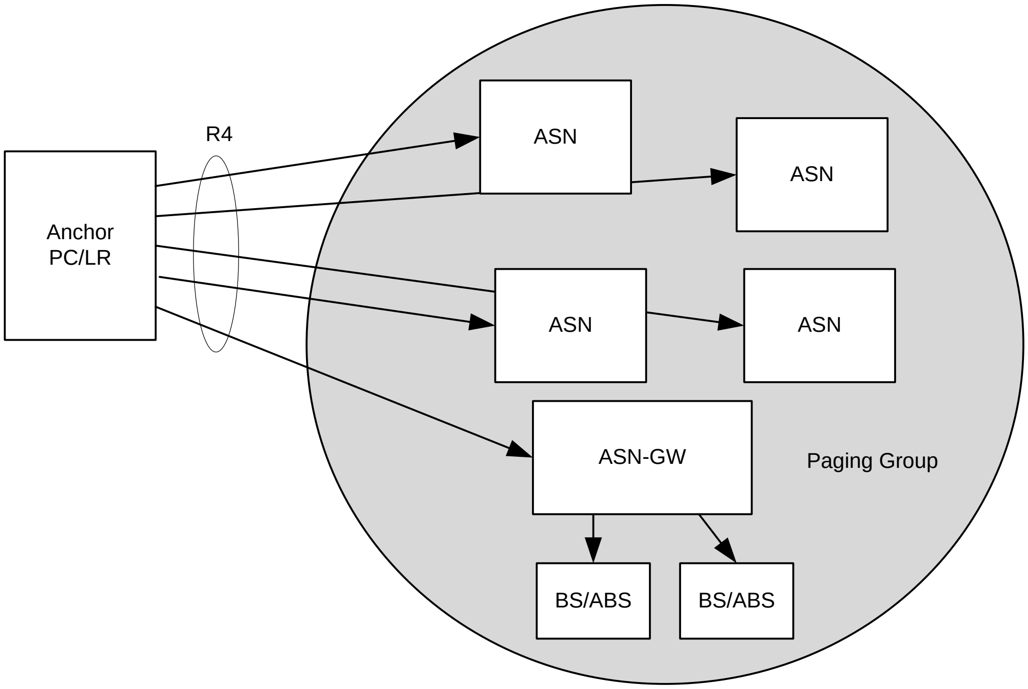


Figure 4-173 – Topologically Aware Paging Announce Scheme

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 4-174). The Anchor PC keeps track of the Relay PC, reported by the last Location Update message received from the MS/AMS. As the MS/AMS 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/AMS 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 BS/ABSs under its control. The additional Relay PC will in turn forward the *Paging_Announce* message to the BS/ABS under 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.

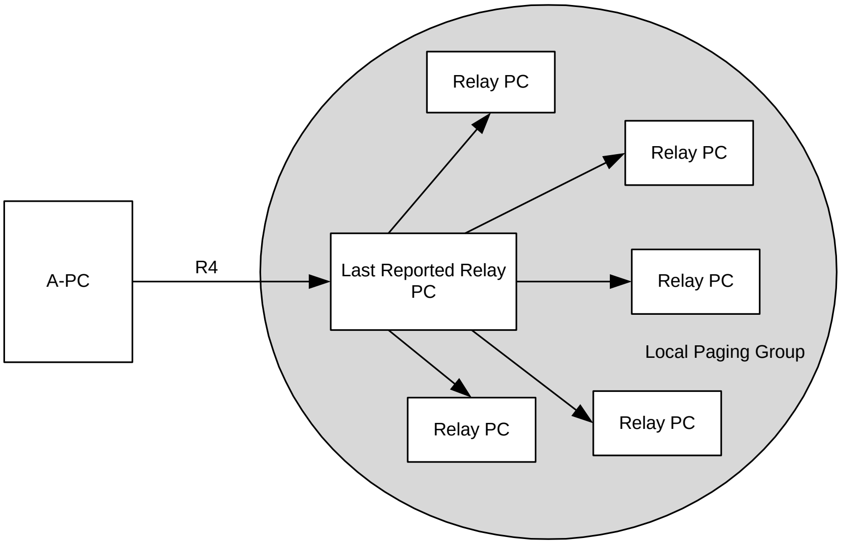


Figure 4-174 – Topologically Unaware Paging Announce Scheme

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 an MS/AMS 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/AMS. 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 BS/ABSs 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/AMS 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/AMS, and additionally it includes a BS ID(s) TLV indicating the BS/ABSs 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 BS/ABSs to be paged. The MS/AMS MAY still be located around the coverage area of the last BS/ABS that performed the last Location Update.

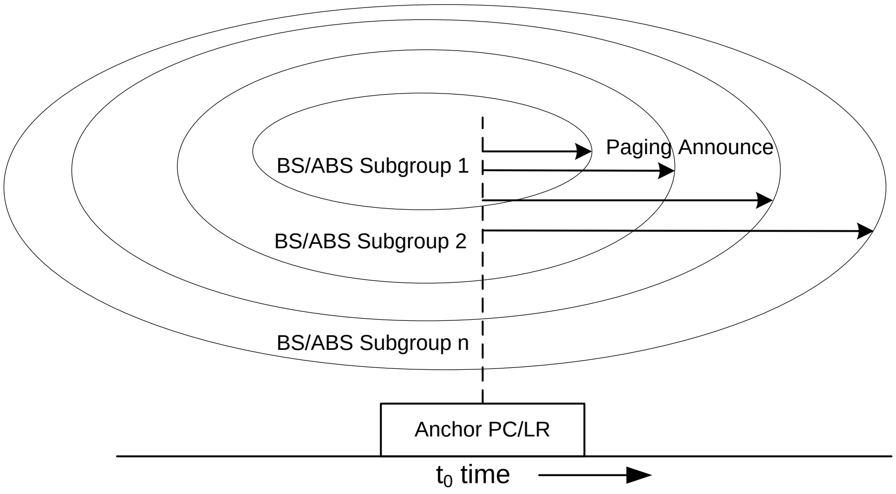


Figure 4-175 – Single-step Paging

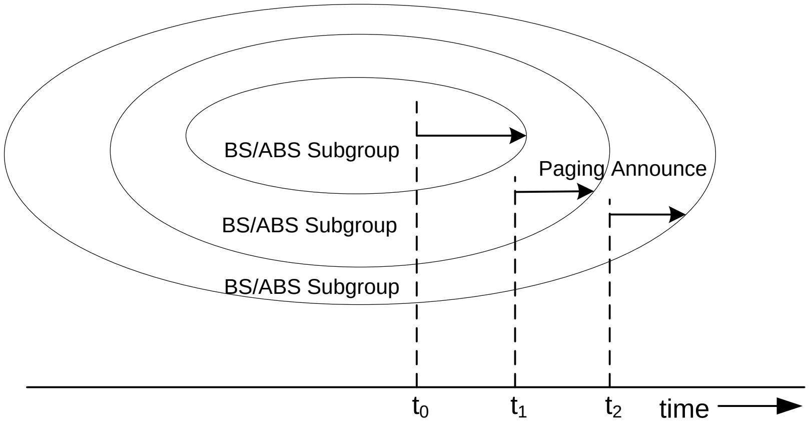


Figure 4-176 – Multi-step Paging

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/AMS or a set of Idle Mode MS/AMS's via the *Paging_Announce* message.

Multicast groups may be created as described in [22]. Each multicast group contains some set of the BS/ABSs – 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 (e.g., DL data arrival for an MS/AMS in Idle mode, Anchor Authenticator reauthentication of an MS/AMS in Idle Mode, etc.), but the paging procedure for each trigger is similar. Figure 4-177 illustrates the paging procedure triggered by DL data arrival (or any other trigger) for an MS/AMS when the MS/AMS is in Idle Mode.

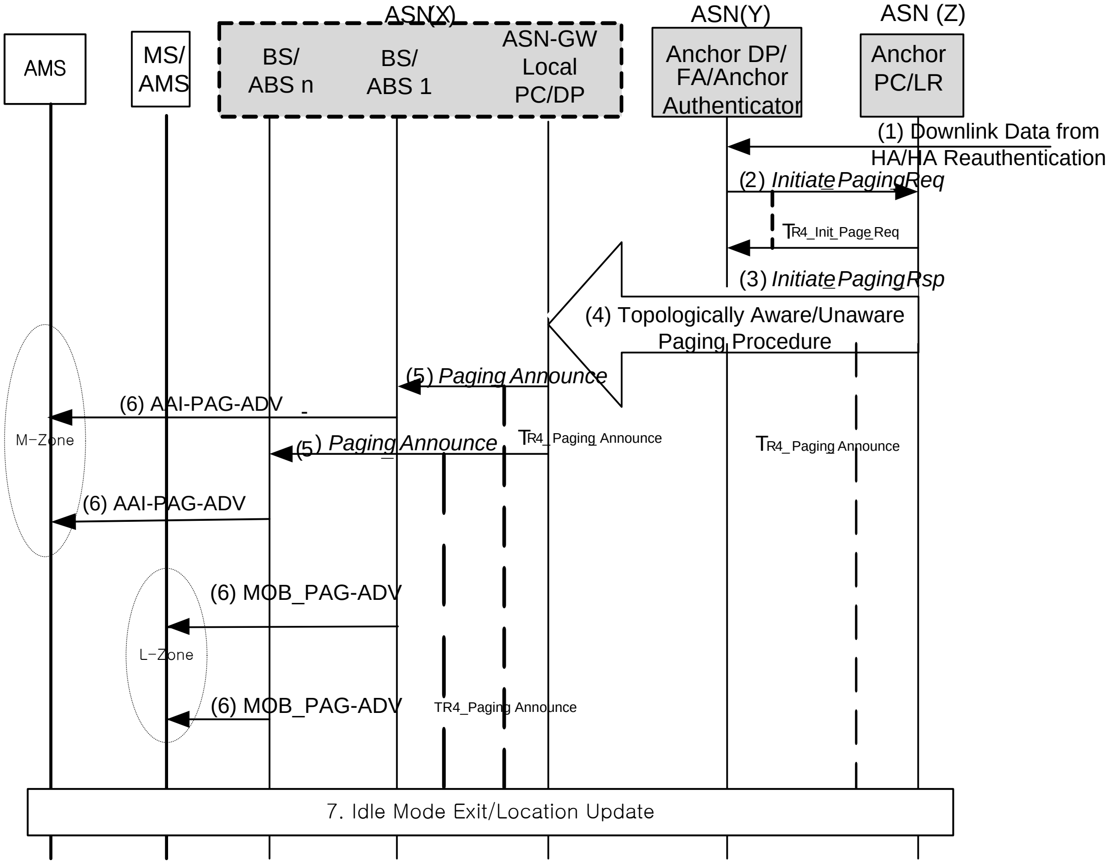


Figure 4-177 – Paging Procedure

STEP 1

Data from HA arrives through the tunnel at the FA and its associated DPF. The Anchor DPF buffers the data. In case that "PMK Grace Time" or "CMAC_KEY_COUNT Grace Interval" is reached, the reauthentication of MS/AMS is initiated. If Anchor Authenticator is not collocated with Anchor DPF, it may activate this MS/AMS.

STEP 2

The Anchor Data Path Function determines that MS/AMS 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 $T_{Init\_Page\_Req}$.

Note1: When MS/AMS is in Idle Mode, if data not belonging to any saved SF of the MS/AMS arrives, the decision to initiate paging or not is left for operator's setting.

Note2: Anchor Authenticator sends an R4 *Initiate_Paging_Req* message to Anchor PC/LR to request paging. The Anchor Authenticator starts timer $T_{Init\_Page\_Req}$.

STEP 3

Anchor PC/LR retrieves the information related to the MS/AMS 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.

Note1: For Anchor Authenticator reauthenticates a MS in Idle Mode case, Anchor PC/LR retrieves the information related to the MS and sends an R4 *Initiate_Paging_Rsp* to Anchor Authenticator. 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/AMS. Upon receipt of this message the Anchor Authenticators stops timer $T_{Init\_Page\_Req}$ if running.

STEP 4

If paging action is authorized, Anchor PC retrieves the MS/AMS 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/ABS(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/ABS from which the MS/AMS performed location update, the Anchor PC SHALL directly issue *Paging_Announce* messages to all, or some subset, of the Paging Group members consisting of BS/ABSs and/or relay PCs in the region.

If the Anchor PC is topologically unaware of the Paging region, or the BS/ABSs 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 BS/ABSs 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 BS/ABSs that belong to the MS Reattachment zone in the *Paging_Announce* message.

If the mobile is an AMS and an M-zone paging is needed, M-Zone *Paging_Announce* message from the Anchor PC includes Paging Cycle, Paging Offset, and advanced air interface TLV of Deregistration ID(DID), to correctly identify the AMS. When more than one MS or AMS need to be paged, the Anchor PC may optimize L-zone paging and M-zone paging by grouping them into separate *Paging_Announce* messages for L-zone and M-zone.

STEP 5

The ASN-GW that contains the local/relay PC function for the MS/AMS initiates the paging operation and sends the R6 *Paging_Announce* message to the relevant BS/ABS(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. The *R6_Paging Announce* message will reflect L-zone paging to BS/ABSs and M-zone paging to ABSs corresponding to the *Paging_Announce* message it received.

STEP 6

Once the Paging Agent (PA) at the BS/ABS receives the *Paging_Announce* message with the requested action set to “Start” it extracts the relevant paging parameters for the MS/AMS (Paging Cycle, Paging Offset) and initiates the paging action requested by sending out MOB-PAG_ADV/AAI-PAG-ADV message over the airlink as per the indicated paging cycle and the paging offset. When the MOB-PAG_ADV message is sent in response to downlink data being received for the MS/AMS which entered idle mode in BS or LZone of ABS, 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/AMS which entered idle mode in BS or LZone of ABS, the Action Code in the message is set to 0b01 (Perform Ranging to establish location and acknowledge message).

When the AAI-PAG_ADV message is sent in response to downlink data being received for the AMS which entered idle mode in MZone of ABS, the Action Code in the message is set to 0b0 (perform network reentry). When the message is sent to trigger a location update from the AMS which entered idle mode in MZone of ABS, the Action Code in the message is set to 0b1 (perform ranging for location update). See IEEE 802.16e section 6.3.2.3.51 and IEEE 802.16m 16.2.3.23.

The optional SF Flow info in the *Paging_Announce* message helps the BS/ABS 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/AMS 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/AMS will perform an Idle Mode Exit or a Location Update procedure. If optional SF Flow info parameters were present in the *Paging_Announce* message for priority treatment, like Emergency Call, ETS priority or just QoS priority, the BS/ABS provides priority for Idle mode Exit or Location Update procedure for the paged MS/AMS. If any Paging Agent (PA) receives a successful reply from the paged MS/AMS, 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/AMS 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 4-178. It is assumed that the MS/AMS is being paged over multiple BS/ABSs (this could be triggered for example either in response to incoming data to be delivered to the MS/AMS 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/AMS (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 BS/ABSs 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.

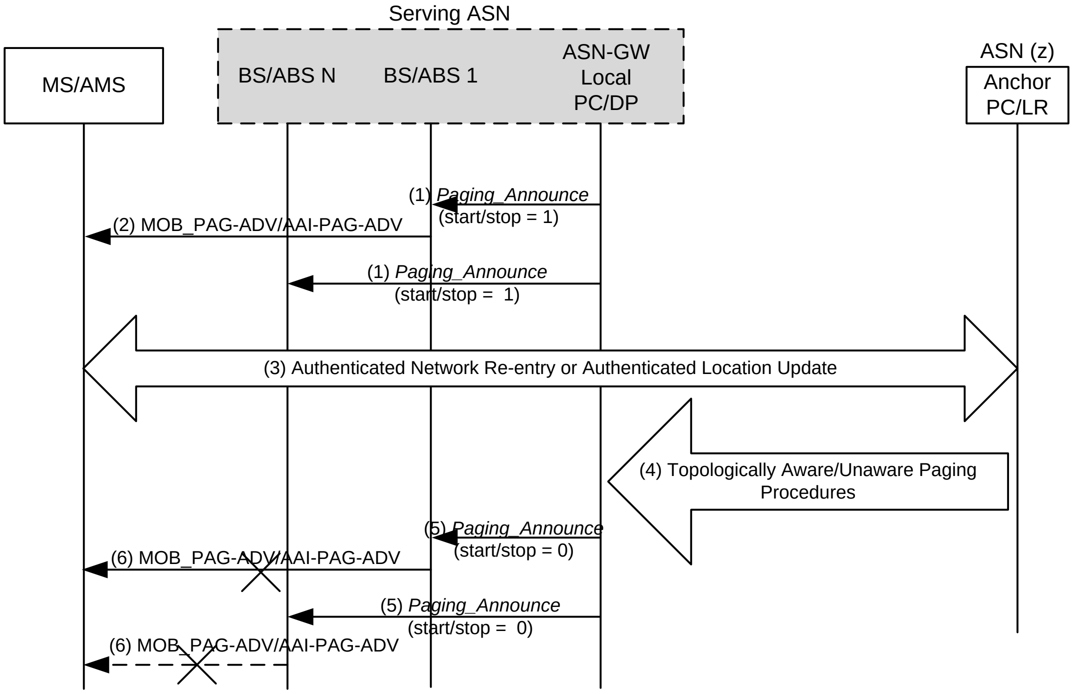

Serving ASN
MS/AMS
BS/ABS N
BS/ABS 1
ASN-GW Local PC/DP
ASN (z)
Anchor PC/LR
(1) Paging_Announce (start/stop = 1)
(2) MOB_PAG-ADV/AAI-PAG-ADV
(1) Paging_Announce (start/stop = 1)
(3) Authenticated Network Re-entry or Authenticated Location Update
(4) Topologically Aware/Unaware Paging Procedures
(5) Paging_Announce (start/stop = 0)
(6) MOB_PAG-ADV/AAI-PAG-ADV
(5) Paging_Announce (start/stop = 0)
(6) MOB_PAG-ADV/AAI-PAG-ADV

Figure 4-178 – Stop Paging Procedure

STEP 1

The Local PC send R6 *Paging_Announce* message to the BS/ABS to initiate paging procedures for the MS/AMS. 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* message from the local PC, the BS/ABS sends a MOB_PAG-ADV/AAI-PAG-ADV message to the MS/AMS. 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/AAI-PAG-ADV, the MS/AMS 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/AMS, the Anchor PC sends a R4 *Paging_Announce* message to all BS/ABSs in the Paging Group. 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 BS/ABSs 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 BS/ABSs. The R6 *Paging_Announce* message has the Paging Start/Stop TLV set to 0.

STEP 6

Once the Paging Agent (PA) at the BS/ABS receives the *Paging_Announce* message with the requested action set to "Stop", it extracts the relevant paging parameters for the MS/AMS (Paging Cycle, Paging Offset and Paging Group ID for Lzone paging. Paging Cycle,Paging Offset, Paging Group ID and Deregistration ID for Mzone paging) and stop sending out MOB-PAG_ADV/AAI-PAG-ADV message over the air link.

The Paging Agent will continue paging the MS/AMS for the duration specified by the Paging Announce Timer TLV, or until the appropriate response is received from the MS/AMS, or until it receives a Paging Stop message for the MS/AMS 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.

When Paging Stop is received at the BS/ABS, any priority given to paging and SF Flow initiation is terminated.

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 4-165 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 4-165 – 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 4-166 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 4-166 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{R4\_Paging\_Announce}$	Anchor PC / Relay PC	The Anchor PC SHALL consider the MS/AMS unavailable and stop paging. The Relay PC has no action.

$T_{R6\_Paging\_Announce}$	Relay PC / Local PC	No action.
$T_{R4\_Init\_Page\_Req}$	Anchor DP Function	Anchor DP Function SHALL discard the stored data for the MS/AMS. 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/AMS, 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/AMS, 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/AMS. The Anchor DP function MAY additionally send some indication to the upstream network elements 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 4-167 – R4 Initiate_Paging_Req

TLV	Reference	M/O	Notes	Applicability
MS Info	5.3.2.103	O		1,2,3
>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.	1,2,3
>>SFID	5.3.2.184	O	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3

Table 4-168 – R4 Initiate_Paging_Rsp

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3
Response Code	5.3.2.153	O	Included in paging not allowed. Valid values: • 0x00 = Not allowed - Paging Reference is zero • 0x01 = Not allowed - No such SF	1,2,3

1 **Table 4-169 – R4 Paging_Announce**

TLV	Reference	M/O	Notes	Applicability
BS Info	5.3.2.26	O		1,2,3
>Reattachment Zone	5.3.2.424	O	Included if the MS mobility access classifier is fixed or nomadic.	1,2,3
>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.	1,2,3
L-BSID	5.3.2.87	O	Last reported BS/ABS included to identify a Paging subgroup. Decision to include this TLV is implementation specific. This is not included for paging stop operation.	1,2,3
Paging Information	5.3.2.119	M	Paging Information TLV obtained from the MS/AMS 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.	1,2,3
>Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS/AMS to be paged which was last stored in Location Register.	1,2,3
>Paging Start/Stop	5.3.2.121	M	1 = start Paging Operation. 0 = stop Paging Operation.	1,2,3
>Paging Announce Timer	5.3.2.115	O	This IE is included for Paging (start) operation. This is not included for paging stop operation.	1,2,3
> Paging Cycle	5.3.2.118	O	This SHALL be mandatory when Paging. Start/Stop = 1.	1,2,3
> Paging Offset	5.3.2.120	O	This SHALL be mandatory when Paging. Start/Stop = 1.	1,2,3
> Paging Interval Length	5.3.2.135	O	This SHALL be mandatory when Paging. Start/Stop = 1 and the MS/AMS entered idle mode in BS or LZone of ABS.	1,2

TLV	Reference	M/O	Notes	Applicability
>Deregistration ID(DID)	5.3.2.480	M	This SHALL be mandatorily together with Paging Group, Paging Offset and Paging Group Id when Paging. Start/Stop = 1 and the AMS entered idle mode in MZone of ABS. Otherwise, it is not included.	3
> Paging Group Id	5.3.2.123	M	This is mandatory if the L-BSID and BSID(s) are not present.	1,2,3
>Paging Cause	5.3.2.116	O	01 = Location update. 02 = Network Re-Entry, Incoming Data for Idle MS, Reauthentication. Other values are reserved. This SHALL be mandatory when Paging Start/Stop = 1.	1,2,3
> Anchor PC ID	5.3.2.12	O		1,2,3
MS Info	5.3.2.103	O		1,2,3
> 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.	1,2,3
>>SFID	5.3.2.184	O	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
> Authenticator ID	5.3.2.19	O	Included as an optimization for reducing the Network entry latency.	1,2,3

1 **Table 4-170 – R6 Paging_Announce**

TLV	Reference	M/O	Notes	Applicability
MS Info	5.3.2.103	O		1,2,3
> 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.	1,2,3
>>SFID	5.3.2.184	O	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
> Authenticator ID	5.3.2.19	O	Included if received in the R4 Paging_Announce message.	1,2,3
Paging Information	5.3.2.119	M	This compound TLV contains Paging	1,2,3

TLV	Reference	M/O	Notes	Applicability
			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 *Paging_Announce* message.	1,2,3
>Paging Start/Stop	5.3.2.121	M	1 = start Paging Operation. 0 = stop Paging Operation.	1,2,3
>Paging Announce Timer	5.3.2.115	O	This IE is included for Paging (start) operation. This is not included for paging stop operation.	1,2,3
> Paging Cycle	5.3.2.118	O	This SHALL be mandatory when Paging. Start/Stop = 1.	1,2,3
> Paging Offset	5.3.2.120	O	This IE is included for Paging (start) operation. This is not included for paging stop operation.	1,2,3
> Paging Interval Length	5.3.2.135	O	This SHALL be mandatory when Paging. Start/Stop = 1 and the MS/AMS entered idle mode in BS or LZone of ABS.	1,2
>Deregistration ID(DID)	5.3.2.480	M	This SHALL be mandatorily together with Paging Group, Paging Offset and Paging Group Id when Paging. Start/Stop = 1 and the AMS entered idle mode in MZone of ABS. Otherwise, it is not included.	3
> Paging Group Id	5.3.2.123	M	This IE is included for Paging (start) operation. This is not included for paging stop operation.	1,2,3
>Paging Cause	5.3.2.116	O	01 = Location update. 02 = Network Re-Entry, Incoming Data for Idle MS, Reauthentication. Other values are reserved. This SHALL be mandatory when Paging Start/Stop = 1.	1,2,3
BS Info	5.3.2.26	O		1,2,3
>BS ID	5.3.2.25	CM		1,2,3

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/AMS exiting idle mode is shown below. Here it is assumed that when the MS/AMS 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/AMS – hence, the entire context has to be retrieved from the Anchor PC. In other words the MS/AMS 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.

In case that MS/AMS which entered idle mode in BS or LZone of ABS performs Idle Mode Exit procedure, the MS/AMS is identified by the MSID. But, in case the AMS entered idle mode in MZone of ABS, the AMS is identified by complete paging information (i.e. uniqueness of the AMS is achieved by the combination of the assigned Paging Group ID + Paging Cycle + Paging Offset + Deregistration ID).

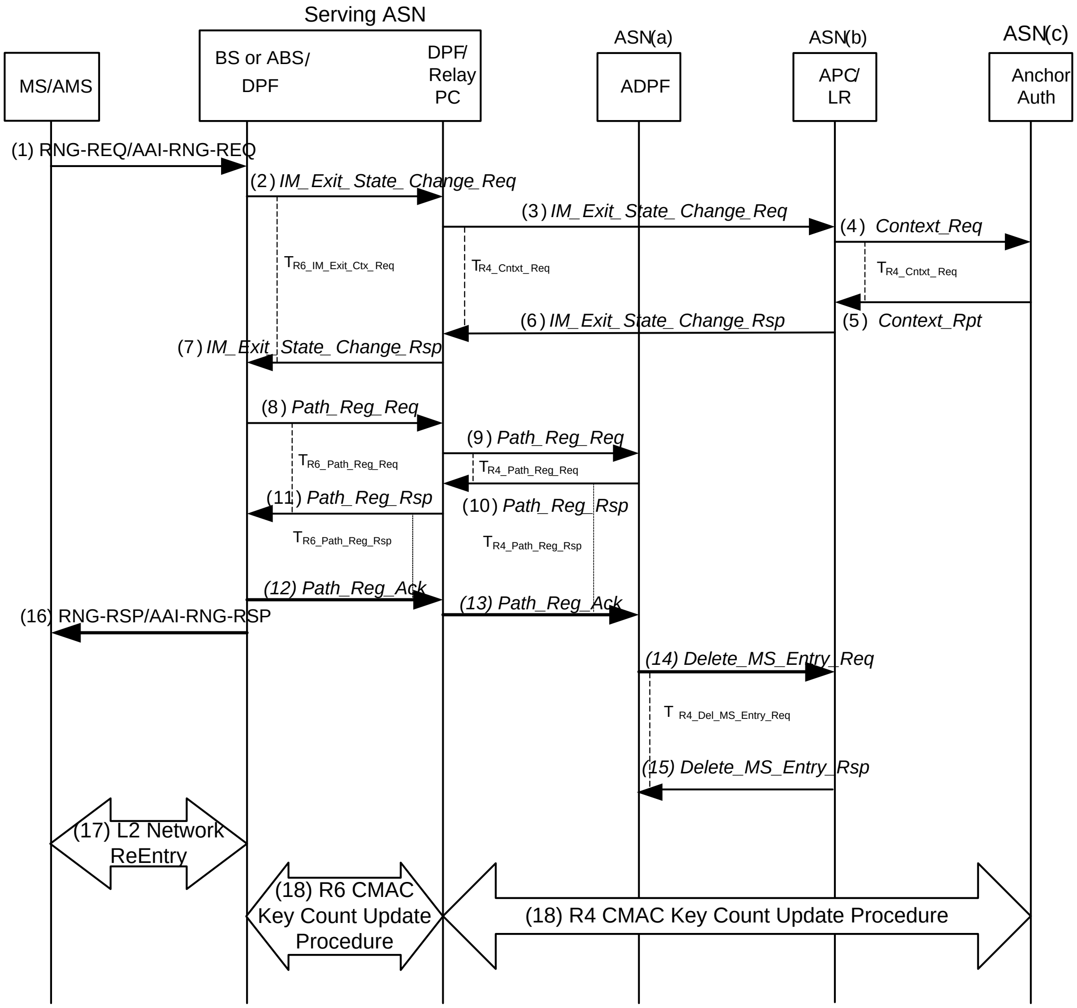


Figure 4-179 – Idle Mode Exit Procedure

Flow Description

MS/AMS 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/AMS exits Idle mode in response to a prior Page message, it performs Ranging (RNG-REQ/AAI-RNG-REQ).

Case b: MS/AMS initiated Idle mode exit

When MS/AMS on its own wants to become active to initiate communication, it performs the steps given below.

STEP 1

MS/AMS initiates exit procedure from IDLE mode and sends RNG_REQ/AAI-RNG-REQ as described in IEEE 802.16 specification.

In the RNG_REG message the Ranging Purpose Indication TLV Bit #0 is set to one and PC ID TLV is included, thus indicating that the MS/AMS intends to Re-Entry from Idle Mode in BS or LZone of ABS.

In the AAI-RNG-REQ message the Ranging Purpose Indication is marked by 0b0010, thus indicating that the AMS intends to Re-Entry from Idle Mode in MZone of ABS.

The BS/ABS receives the RNG_REQ/AAI-RNG-REQ message from MS/AMS indicating Idle mode exit and sends R6 *IM_Exit_State_Change_Req* to the Relay PC in the ASN-GW, indicating that the MS/AMS wants to become active. Timer $T_{R6\_IM\_Exit\_Ctx\_Req}$ is started at this point by the BS/ABS to monitor the response for this message.

STEP 2

The Relay PC in the Serving ASN receives the R6 *IM_Exit_State_Change_Req* from the BS/ABS indicating Idle mode exit and sends R4 *IM_Exit_State_Change_Req* to the Anchor PC/LR in ASN(b), indicating that the MS/AMS 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/ABS ID belongs to the MS Reattachment Zone. Only if the Serving BS/ABS ID belongs to the MS Reattachment Zone, the Anchor PC proceeds with step 4, otherwise it proceeds with step 6 to direct the MS/AMS to do initial network entry.

STEP 3

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 4

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 5

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/AMS at the Anchor PC.

STEP 6

Serving ASN retrieves the MS context from Anchor PC ASN and forwards the MS context to the BS/ABS on the R6 interface. Once the BS/ABS 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/AAI-RNG-REQ message.

STEP 7

After successful RNG-REQ/AAI-RNG-REQ authentication, the BS/ABS 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/ABS to monitor the response for this message.

STEP 8

The Serving ASN extends the data path establishment to the FA or Anchor DPF in ASN(a) across the R4 interfaces.

STEP 9

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 10

The DPF in the serving ASN confirms data path establishment - sends R6 *Path_Reg_Rsp* to the Serving BS/ABS. Also, once the BS/ABS receives this message, Timer $T_{R6\_Path\_Reg\_Req}$ is stopped.

STEP 11

The BS/ABS sends R6 *Path_Reg_Ack* to the Data Path function in the serving ASN.

STEP 12

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 13

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/AMS. If MS/AMS 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 14

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.

STEP 15

After successful RNG-REQ/AAI-RNG-REQ authentication, the BS/ABS will use MS service and operational information indicated by IDLE Mode Retain Info obtained by Step 7 to construct HO Process Optimization /Reentry Process Optimization TLV (802.16e/m parameter) settings in the RNG-RSP/AAI-RNG-RSP based on local policy; then sends RNG_RSP/AAI-RNG-RSP message to the MS/AMS formatted according to IEEE 802.16e/m specification. This message delivers all the required information to resume service in accordance with Idle Mode Retain Information.

The BS/ABS may trigger this step immediately after the step 7, before or in parallel to steps 8-13 (Path Registration transaction with MS/AMS' Anchor GW/ ADPF). This is the BS/ABS local implementation decision.

STEP 16

The MS/AMS completes Network Re-Entry from the Idle Mode as described in IEEE 802.16e/m specification (immediately following the previous step).

STEP 17

After the MS/AMS successfully completes Network Re-entry from IM (as indicated in the previous step), the BS/ABS updates the Anchor Authenticator with the CMAC Key count for the MS/AMS 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 4.10.5.9. The Anchor Authenticator acknowledges the CMAC update for the MS/AMS.

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 4-171 employs the following timers:

- $T_{R6\_IM\_Exit\_Ctx\_Req}$: is started by a BS/ABS 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/ABS 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 4-171 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 4-171 – 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 4-172 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 4-172 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{R6\_IM\_Exit\_Ctx\_Req}$	BS/ABS	RNG-RSP/AAI-RNG-RSP message indicating that IM Exit is not possible is sent to the MS/AMS on the air interface.
$T_{R4Cntxt\_Req}$	Anchor PC	Anchor PC indicates to the Relay PC, failure of context retrieval for the MS/AMS in the *IM_Exit_State_Change_Rsp* message.
$T_{R6\_Path\_Reg\_Req}$	BS DPF	RNG-RSP/AAI-RNG-RSP message indicating that IM Exit is not possible is sent to the MS/AMS 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/AMS in the R4 *Path_Reg_Rsp* 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/ABS which sends the appropriate failure code to the MS/AMS on R1 via RNG-RSP/AAI-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/ABS. The BS, upon receipt of the message, sends the appropriate failure code to the MS/AMS on R1 via RNG-RSP/AAI-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/ABS which sends the appropriate failure code to the MS/AMS on R1 via RNG-RSP/AAI-RNG-RSP message.

4.10.4.1.2.5 Serving BS/ABS 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/ABS ID belongs to the MS Reattachment Zone.

If the MS mobility access classifier is fixed or nomadic, the MS/AMS' Authenticator SHALL reject context requests retrieval for the unauthorized BS/ABS based on Authenticator's knowledge of MS Reattachment list. To reject the context request, the MS/AMS' Authenticator responds to Anchor PC with *Context-Rpt* message that includes appropriate Failure Indication value and excludes MS/AMS' AK context.

If the Serving BS/ABS 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/ABS is out of MS Reattachment Zone. Then the BS/ABS will send the appropriate failure code to the MS/AMS on R1 via RNG-RSP/AAI-RNG-RSP message directing the MS/AMS to initial network entry.

4.10.4.2 Idle Mode Exit – Serving ASN Has MS Context

As per IEEE 802.16e/m, when the MS/AMS enters idle mode, the BS/ABS in the serving ASN starts a timer – "Management Resource Holding Timer". The BS/ABS retains all of the R1 context and the R4, R6 data paths for this MS/AMS 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/ABS to revoke the MS context if the MS/AMS has entered the network at a different BS/ABS before the management resource holding timer at the serving BS/ABS expires. How the anchor PC determines whether the management resource holding timer has expired at the serving BS/ABS is an implementation issue.

If the context in the serving BS/ABS is not revoked before the management resource holding timer expires, the serving BS/ABS SHALL release the MS context and the data paths for this MS/AMS only at the expiry of this timer.

In certain cases the MS/AMS may decide to exit idle mode before this timer expires and/or before the MS context is revoked from the serving BS/ABS. In such a case, the procedure for the MS/AMS to exit idle mode can be further simplified and is illustrated in Figure 4-180.

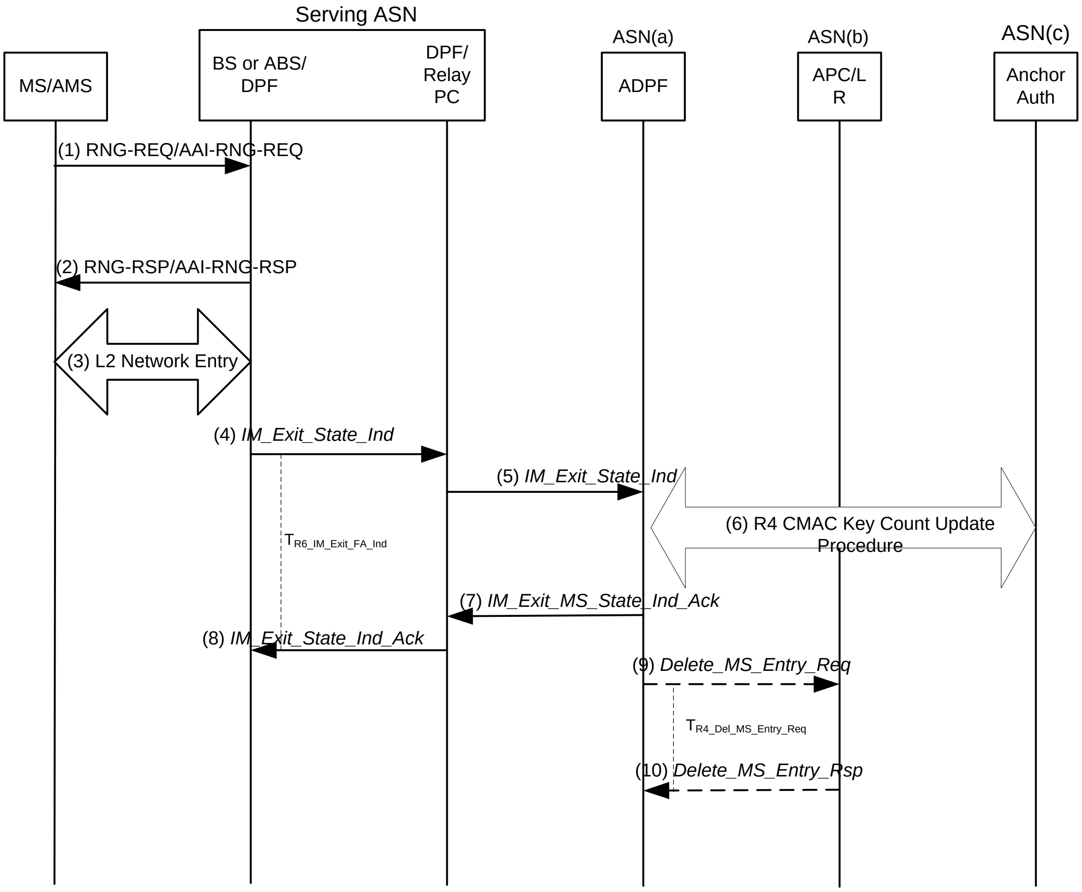


Figure 4-180 – Idle Mode Exit Procedure when the Management Resource Holding Timer has not Expired and when the MS State Stored at the BS/ABS is not Revoked by the Anchor PC

The steps in the above procedure are detailed below:

STEP 1

The MS/AMS sends an RNG-REQ/AAI-RNG-REQ to enter back into the network from Idle mode before the timer expires.

STEP 2

The BS/ABS has the required context now and the data paths retained for this MS/AMS since Management Resource Holding Timer is not expired. Hence it authenticates the MS/AMS and sends RNG-RSP/AAI-RNG-RSP back to the MS/AMS.

STEP 3

The MS/AMS completes Network Re-Entry from the Idle Mode as described in IEEE 802.16e/m specification.

STEP 4

The BS/ABS SHALL send R6 *IM_Exit_State_Ind* to the DPF in the serving ASN-GW to indicate the MS/AMS 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 $T_{R6\_IM\_Exit\_FA\_Ind}$ is started at this point by the BS/ABS 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/AMS 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/ABS. Once the BS/ABS 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/AMS 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/AMS 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 4-173 employs the following timers:

- $T_{R6\_IM\_Exit\_FA\_Ind}$: is started by a BS/ABS 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 4-173 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 4-173 – 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 4-174 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 4-174:

Table 4-174 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{R6\_IM\_Exit\_FA\_Ind}$	BS/ABS	RNG-RSP/AAI-RNG-RSP message indicating that IM Exit is not possible is sent to the MS/AMS on the air interface.
$T_{R4\_Del\_MS\_Entry\_Req}$	Anchor ASN DPF	No action required.

4.10.4.2.2.2 MS/AMS CMAC Validation Failure

In case, CMAC validation failure occurs at BS/ABS, it SHALL send the appropriate failure indication TLV in the RNG_RSP/AAI-RNG-RSP to the MS/AMS. It SHALL then initiate Data Path tear down by sending Data Path Dereg Req.

4.10.4.3 IM Exit Message Tables

Table 4-175 – IM_Exit_State_Change_Req over R6

TLV	Reference	M/O	Notes	Applicability
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	ID of the BS/ABS from which MS/AMS is initiating Idle mode Exit.	1,2,3
Paging Information	5.3.2.119	M		1,2,3
> current Paging Cycle	5.3.2.481	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
> current Paging Offset	5.3.2.482	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
> current Deregistration ID	5.3.2.483	M	Deregistration ID assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
>current Paging Group ID	5.3.2.484	M	Paging Group ID assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
>Anchor PC ID	5.3.2.12	M	PC ID points to MS/AMS's anchor Paging Controller, as obtained from the RNG-REQ/AAI-RNG-REQ message.	1,2,3

Table 4-176 – IM_Exit_State_Change_Rsp over R6

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Code value = 32. Included in the event of failure.	1,2,3
BS Info	5.3.2.26	M		1,2,3
> BS ID	5.3.2.25	M	ID of the BS/ABS from which MS/AMS is initiating Idle mode Exit.	1,2,3
> AK Context	5.3.2.6	M	AK, AKID, Lifetime, AK Sequence.	1,2,3
>>AK	5.3.2.5	M		1,2,3
>>AK ID	5.3.2.7	M		1,2,3
>>AK Lifetime	5.3.2.8	M		1,2,3
>>AK SN	5.3.2.9	M		1,2,3
>>CMAC_KEY_COUNT	5.3.2.34	M		1,2,3

TLV	Reference	M/O	Notes	Applicability
Paging Information	5.3.2.119	M		1,2,3
>IDLE Mode Retain Info	5.3.2.81	M	IDLE Mode Retain Info.	1,2,3
MS Info	5.3.2.103	M		1,2,3
> MSID	5.3.2.102	M	MSID SHALL be included for the case ONLY for AMS which entered idle mode in MZone of ABS.	3
>CRID	5.3.2.475	M		3
>Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS/AMS. 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/AMS 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.	1,2,3
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1,2,3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1,2,3
>SBC context	5.3.2.174	M		1,2,3
>>HARQ Context (one or more)	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>Direction	5.3.2.59	O	Indicates the direction of the management connection.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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	1,2

TLV	Reference	M/O	Notes	Applicability
>>Subscriber Transition Gaps	5.3.2.316	M	See IEEE802.16e for further details.	1,2
>>Maximum Transmit Power	5.3.2.317	M	See IEEE802.16e/m for further details.	1,2,3
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	M	See IEEE802.16e for further details.	1,2
>>PKM Flow Control	5.3.2.319	M	See IEEE802.16e for further details.	1,2
>>Maximum Number of Supported Security Associations	5.3.2.320	M	See IEEE802.16e for further details.	1,2
>>Security Negotiation Parameters	5.3.2.321	M	See IEEE802.16e/m for further details.	1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2,3
>>>Authorization Policy Support	5.3.2.21	M	See IEEE802.16e/m for further details.	1,2,3
>>>MAC Mode	5.3.2.322	M	See IEEE802.16e for further details.	1,2
>>>PN Window Size	5.3.2.324	M	See IEEE802.16e/m for further details.	1,2,3
>>Association type support	5.3.2.465	O		1,2
>>>Size of ICV	5.3.2.502	M	See IEEE802.16m for further details.	3
>>Extended Subheader Capability	5.3.2.325	M	See IEEE802.16e for further details.	1,2
>>HO Trigger Metric Support	5.3.2.326	M	See IEEE802.16e for further details.	1,2
>>Current Transmit Power	5.3.2.327	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	M	See IEEE802.16e/m for further details.	1,2,3
>>OFDMA SS demodulator	5.3.2.329	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS modulator	5.3.2.330	M	See IEEE802.16e for further details.	1,2
>>The number of UL HARQ Channel	5.3.2.331	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Permutation support	5.3.2.332	M	See IEEE802.16e for further details.	1,2

TLV	Reference	M/O	Notes	Applicabili ty
>>OFDMA SS CINR Measurement Capability	5.3.2.333	M	See IEEE802.16e for further details.	1,2
>>The number of DL HARQ Channels	5.3.2.334	M	See IEEE802.16e for further details.	1,2
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Uplink Power Control Support	5.3.2.336	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	M	See IEEE802.16e for further details.	1,2
>>OFDMA MAP Capability	5.3.2.338	M	See IEEE802.16e for further details.	1,2
>>Uplink Control Channel Support	5.3.2.339	M	See IEEE802.16e for further details.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	M	See IEEE802.16e for further details.	1,2
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS modulator for MIMO Support	5.3.2.343	M	See IEEE802.16e for further details.	1,2
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	M	See IEEE802.16e for further details.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O	See IEEE802.16m for further details.	3
>>DEVICE_CLASS	5.3.2.504	O	See IEEE802.16m for further details.	3
>>CLC Request	5.3.2.505	O	See IEEE802.16m for further details.	3
>>Long TTI for DL	5.3.2.506	O	See IEEE802.16m for further details.	3
>>UL sounding	5.3.2.507	O	See IEEE802.16m for further details.	3
>>OL Region	5.3.2.508	O	See IEEE802.16m for further details.	3
>>DL resource metric for	5.3.2.509	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
FFR				
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O	See IEEE802.16m for further details.	3
>>DL MIMO mode	5.3.2.512	O	See IEEE802.16m for further details.	3
>>feedback support for DL	5.3.2.513	O	See IEEE802.16m for further details.	3
>>Subband assignment A-MAP IE support	5.3.2.514	O	See IEEE802.16m for further details.	3
>>DL pilot pattern for MU MIMO	5.3.2.515	O	See IEEE802.16m for further details.	3
>>Number of Tx antenna of AMS	5.3.2.516	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O	See IEEE802.16m for further details.	3
>>UL pilot pattern for MU MIMO	5.3.2.519	O	See IEEE802.16m for further details.	3
>>UL MIMO mode	5.3.2.520	O	See IEEE802.16m for further details.	3
>>Modulation scheme	5.3.2.521	O	See IEEE802.16m for further details.	3
>>UL HARQ buffering capability	5.3.2.522	O	See IEEE802.16m for further details.	3
>>DL HARQ buffering capability	5.3.2.523	O	See IEEE802.16m for further details.	3
>>AMS DL processing capability per sub-frame	5.3.2.524	O	See IEEE802.16m for further details.	3
>>AMS UL processing capability per sub-frame	5.3.2.525	O	See IEEE802.16m for further details.	3
>>FFT size(2048/1024/512)	5.3.2.526	O		3
>>Authorization policy support	5.3.2.21	O		3
>>Inter-RAT Operation Mode	5.3.2.527	O		3
>>Supported Inter-RAT type	5.3.2.528	O		3

TLV	Reference	M/O	Notes	Applicability
>>MIH Capability Supported	5.3.2.529	O		3
> REG context	5.3.2.144	O		1,2,3
>>Number of UL Transport CIDs Support	5.3.2.288	M	See IEEE802.16e for further details.	1,2
>>Number of DL Transport CIDs Support	5.3.2.289	M	See IEEE802.16e for further details.	1,2
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	M	See IEEE802.16e/m for further details. It is named as 'CS type support' in 16m.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	M	See IEEE802.16e/m for further details.	1,2,3
>>PHS Support	5.3.2.292	M	See IEEE802.16e/m for further details.	1,2,3
>>ARQ Support	5.3.2.293	M	See IEEE802.16e for further details. For 16m the value may be set by 1(i.e. ARQ is supported).	1,2
>>DSx Flow Control	5.3.2.294	M	See IEEE802.16e for further details.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>Maximum MAC Data per Frame Support	5.3.2.296	M	See IEEE802.16e for further details.	1,2
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	M	See IEEE802.16e for further details.	1,2
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	M	See IEEE802.16e for further details.	1,2
>>Packing Support	5.3.2.299	M	See IEEE802.16e for further details. For 16m the value may be set by 1(i.e. packing supported).	1,2
>>MAC ertPS Support	5.3.2.300	M	See IEEE802.16e for further details. For 16m the value may be set by 1(i.e. ertPS supported).	1,2
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	M	See IEEE802.16e for further details.	1,2
>>HO Supported	5.3.2.302	M	See IEEE802.16e for further details.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	M	See IEEE802.16e for further details.	1,2

TLV	Reference	M/O	Notes	Applicability
>>Mobility Features Supported	5.3.2.304	M	See IEEE802.16e for further details.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	M	See IEEE802.16e for further details.	1,2
>>Idle Mode Timeout	5.3.2.268	M	See IEEE802.16e for further details.	1,2
>>ARQ Ack Type	5.3.2.307	M	See IEEE802.16e for further details.	1,2
>>MS HO Connections Parameters Proc Time	5.3.2.308	M	See IEEE802.16e for further details.	1,2
>>MS HO TEK Proc Time	5.3.2.309	M	See IEEE802.16e for further details.	1,2
>>MAC Header and Extended Sub-Header Support	5.3.2.310	M	See IEEE802.16e for further details.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	M	See IEEE802.16e for further details.	1,2
>>BS Switching Timer	5.3.2.314	M	See IEEE802.16e for further details.	1,2
>>Power Saving Class Capability	5.3.2.315	M	See IEEE802.16e for further details.	1,2
>>MAXIMUM_ARQ_ BUFFER_SIZE	5.3.2.532	O	See IEEE802.16m for further details.	3
>>MAXIMUM_NON_ ARQ_BUFFER_SIZE	5.3.2.533	O	See IEEE802.16m for further details.	3
>>Multicarrier capabilities	5.3.2.485	O	See IEEE802.16m for further details.	3
>>Zone Switch Mode Support	5.3.2.486	O	See IEEE802.16m for further details.	3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O	See IEEE802.16m for further details.	3
>>Interference mitigation supported	5.3.2.488	O	See IEEE802.16m for further details.	3
>>E-MBS capabilities	5.3.2.489	O	See IEEE802.16m for further details.	3
>>Channel BW and Cyclic prefix	5.3.2.490	O	See IEEE802.16m for further details.	3
>>frame configuration to support legacy R1.0	5.3.2.491	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
>>Persistent Allocation support	5.3.2.492	O	See IEEE802.16m for further details.	3
>>Group Resource Allocation support	5.3.2.493	O	See IEEE802.16m for further details.	3
>>Co-located coexistence capability support	5.3.2.494	O	See IEEE802.16m for further details.	3
>>HO Trigger Metric Support	5.3.2.326	O	See IEEE802.16m for further details.	3
>>EBB Handover support	5.3.2.495	O	See IEEE802.16m for further details.	3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O	See IEEE802.16m for further details.	3
>>Capability for sounding antenna switching support	5.3.2.497	O	See IEEE802.16m for further details.	3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O	See IEEE802.16m for further details.	3
>>ROHC support	5.3.2.499	O	See IEEE802.16m for further details.	3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O	See IEEE802.16m for further details.	3
>Authenticator ID	5.3.2.19	M	Anchor Authenticator of the MS/AMS.	1,2,3
>Anchor ASN GW ID	5.3.2.10	M	Anchor DPF/FA of the MS/AMS.	1,2,3
>SF Info	5.3.2.185	M		1,2,3
>>SFID	5.3.2.184	M		1,2,3
>>SF Type	5.3.2.306	O		1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>PDU SN extended	5.3.2.456	O	Specifies if PDU SN extended subheader	1,2

TLV	Reference	M/O	Notes	Applicability
subheader for HARQ reordering			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		1,2,3
>>CS Type	5.3.2.39	O	This TLV is included in the transmitted message for the target ASN to setup flow.	1,2,3
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.	1,2,3
>>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.	1,2,3
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1,2,3
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_SYNC_LOSS_TIMEOUT	5.3.2.350	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_BLOCK_SIZE	5.3.2.353	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>SN Feedback Enabled field	5.3.2.468	O		1,2
>>FSN Size	5.3.2.469	O		1,2
>>>ARQ_SUB_BLOC	5.3.2.531	O	This TLV SHALL be included if ARQ	3

TLV	Reference	M/O	Notes	Applicability
K_SIZE			Context is included in the transmitted message.	
>>>ARQ_ERROR_DETECTION_TIMEOUT	5.3.2.534	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_FEEDBACK_POLL_RETRY_TIMEOUT	5.3.2.535	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>CID	5.3.2.29	O		1,2
>>FID	5.3.2.471	O		3
>>SAID	5.3.2.169	O		1,2,3
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O		1,2,3
>>>Classification Rule Index	5.3.2.30	O	Index assigned to the Packet Classification Rule.	1,2,3
>>> Classification Rule Priority	5.3.2.32	O		1,2,3
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...	1,2,3
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.	1,2,3
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.	1,2,3
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.	1,2,3
>>>IPv6 Flow Label	5.3.2.470	O		1,2,3
>>QoS Parameters	5.3.2.141	M		1,2,3
>>> DSCP	5.3.2.409	O	TC bit set to 1	1,2,3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	This TLV may be included if BE Data	1,2,3

TLV	Reference	M/O	Notes	Applicability
			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.	1,2,3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	This TLV may be included if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	This TLV may be included if NRT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>RT-VR Data	5.3.2.165	O	Set to RT-VR delivery service.	1,2,3

TLV	Reference	M/O	Notes	Applicability
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.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	This TLV may be included if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	This TLV may be included if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3

TLV	Reference	M/O	Notes	Applicability
>>>>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.	1,2,3
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1,2,3
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1,2,3
>>>Media Flow Type	5.3.2.94	O		1,2,3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1,2,3
>>>Reduced Resources Code	5.3.2.237	O		1,2,3
>>PHS Rule	5.3.2.127	O		1,2,3
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSF	0	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
> 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	1,2,3
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Older TEK	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted	1,2

TLV	Reference	M/O	Notes	Applicability
Parameters			message.	
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>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.	1,2,3
>Reattachment-Zone	5.3.2.424	O	Shall be included by the BS if the MS mobility access classifier is included.	1,2,3
Paging Information	5.3.2.119	M	SHALL be included to identify AMS as obtained from the AAI-RNG-REQ message.	3
> current Paging Cycle	5.3.2.481	M	Parameter which was assigned to AMS by	3

TLV	Reference	M/O	Notes	Applicability
			anchor PC as obtained from the AAI-RNG-REQ message.	
> current Paging Offset	5.3.2.482	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
> current Deregistration ID	5.3.2.483	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
>current Paging Group ID	5.3.2.484	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3

1 **Table 4-177 – Path_Reg_Ack over R6**

TLV	Description	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS/ABS. performing operation. Included during IM Mode Exit procedure.	1,2,3
> Serving/Target Indicator	5.3.2.182	M	Set to “Serving”.	1,2,3

2 **Table 4-178 – IM_Exit_State_Change_Req over R4**

TLV	Reference	M/O	Notes	Applicability
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	ID of the BS/ABS from which MS/AMS is initiating Idle mode Exit.	1,2,3
Paging Information	5.3.2.119	M		1,2,3
> current Paging Cycle	5.3.2.481	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
> current Paging Offset	5.3.2.482	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
> current Deregistration ID	5.3.2.483	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3

> current Paging Group ID	5.3.2.484	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
> Anchor PC ID	5.3.2.12	M	PC ID points to MS/AMS's anchor Paging Controller, as obtained from the RNG-REQ/AAI-RNG-REQ.	1,2,3

1 **Table 4-179 – IM_Exit_State_Change_Rsp over R4**

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Code value = 32. Included in the event of failure.	1,2,3
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	ID of the BS/ABS from which MS/AMS is initiating Idle mode Exit.	1,2,3
>AK Context	5.3.2.6	M	AK, AKID, Lifetime, AK Sequence.	1,2,3
>>AK	5.3.2.5	M		1,2,3
>>AK ID	5.3.2.7	M		1,2,3
>>AK Lifetime	5.3.2.8	M		1,2,3
>>AK SN	5.3.2.9	M		1,2,3
>>CMAC_KEY_COUNT	5.3.2.34	M		1,2,3
MS Info	5.3.2.103	M		1,2,3
> MSID	5.3.2.102	M	MSID SHALL be included for the case ONLY for AMS which entered idle mode in MZone of ABS.	3
>CRID	5.3.2.475	M		3
>Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS/AMS. 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/AMS 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.	1,2,3
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1,2,3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included	1,2,3

TLV	Reference	M/O	Notes	Applicability
			in the transmitted message.	
>SBC Context	5.3.2.174	M		1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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.	1,2
>>Subscriber Transition Gaps	5.3.2.316	M	See IEEE802.16e for further details.	1,2
>>Maximum Transmit Power	5.3.2.317	M	See IEEE802.16e/m for further details.	1,2,3
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	M	See IEEE802.16e for further details.	1,2
>>PKM Flow Control	5.3.2.319	M	See IEEE802.16e for further details.	1,2
>>Maximum Number of Supported Security Associations	5.3.2.320	M	See IEEE802.16e for further details.	1,2
>>Security Negotiation Parameters	5.3.2.321	M	See IEEE802.16e/m for further details.	1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2,3
>>>Authorization Policy Support	5.3.2.21	M	See IEEE802.16e/m for further details.	1,2,3
>>>MAC Mode	5.3.2.322	M	See IEEE802.16e for further details.	1,2
>>>PN Window Size	5.3.2.324	M	See IEEE802.16e/m for further details.	1,2,3
>>Association type support	5.3.2.465	O		1,2
>>>Size of ICV	5.3.2.502	M	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
>>Extended Subheader Capability	5.3.2.325	M	See IEEE802.16e for further details.	1,2
>>HO Trigger Metric Support	5.3.2.326	M	See IEEE802.16e for further details.	1,2
>>Current Transmit Power	5.3.2.327	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	M	See IEEE802.16e/m for further details.	1,2,3
>>OFDMA SS demodulator	5.3.2.329	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS modulator	5.3.2.330	M	See IEEE802.16e for further details.	1,2
>>The number of UL HARQ Channel	5.3.2.331	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Permutation support	5.3.2.332	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS CINR Measurement Capability	5.3.2.333	M	See IEEE802.16e for further details.	1,2
>>The number of DL HARQ Channels	5.3.2.334	M	See IEEE802.16e for further details.	1,2
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Uplink Power Control Support	5.3.2.336	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	M	See IEEE802.16e for further details.	1,2
>>OFDMA MAP Capability	5.3.2.338	M	See IEEE802.16e for further details.	1,2
>>Uplink Control Channel Support	5.3.2.339	M	See IEEE802.16e for further details.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	M	See IEEE802.16e for further details.	1,2
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS	5.3.2.343	M	See IEEE802.16e for further details.	1,2

TLV	Reference	M/O	Notes	Applicability
modulator for MIMO Support				
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	M	See IEEE802.16e for further details.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O	See IEEE802.16m for further details.	3
>>DEVICE_CLASS	5.3.2.504	O	See IEEE802.16m for further details.	3
>>CLC Request	5.3.2.505	O	See IEEE802.16m for further details.	3
>>Long TTI for DL	5.3.2.506	O	See IEEE802.16m for further details.	3
>>UL sounding	5.3.2.507	O	See IEEE802.16m for further details.	3
>>OL Region	5.3.2.508	O	See IEEE802.16m for further details.	3
>>DL resource metric for FFR	5.3.2.509	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O	See IEEE802.16m for further details.	3
>>DL MIMO mode	5.3.2.512	O	See IEEE802.16m for further details.	3
>>feedback support for DL	5.3.2.513	O	See IEEE802.16m for further details.	3
>>Subband assignment A-MAP IE support	5.3.2.514	O	See IEEE802.16m for further details.	3
>>DL pilot pattern for MU MIMO	5.3.2.515	O	See IEEE802.16m for further details.	3
>>Number of Tx antenna of AMS	5.3.2.516	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O	See IEEE802.16m for further details.	3
>>UL pilot pattern for MU MIMO	5.3.2.519	O	See IEEE802.16m for further details.	3
>>UL MIMO mode	5.3.2.520	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
>>Modulation scheme	5.3.2.521	O	See IEEE802.16m for further details.	3
>>UL HARQ buffering capability	5.3.2.522	O	See IEEE802.16m for further details.	3
>>DL HARQ buffering capability	5.3.2.523	O	See IEEE802.16m for further details.	3
>>AMS DL processing capability per sub-frame	5.3.2.524	O	See IEEE802.16m for further details.	3
>>AMS UL processing capability per sub-frame	5.3.2.525	O	See IEEE802.16m for further details.	3
>>FFT size(2048/1024/512)	5.3.2.526	O	See IEEE802.16m for further details.	
>>Authorization policy support	5.3.2.21	O	See IEEE802.16m for further details.	3
>>Inter-RAT Operation Mode	5.3.2.527	O	See IEEE802.16m for further details.	3
>>Supported Inter-RAT type	5.3.2.528	O	See IEEE802.16m for further details.	3
>>MIH Capability Supported	5.3.2.529	O	See IEEE802.16m for further details.	3
>REG context	5.3.2.144	O		1,2,3
>>Number of UL Transport CIDs Support	5.3.2.288	M	See IEEE802.16e for further details.	1,2
>>Number of DL Transport CIDs Support	5.3.2.289	M	See IEEE802.16e for further details.	1,2
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	M	See IEEE802.16e for further details.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	M	See IEEE802.16e for further details.	1,2,3
>>PHS Support	5.3.2.292	M	See IEEE802.16e for further details.	1,2,3
>>ARQ Support	5.3.2.293	M	See IEEE802.16e for further details.	1,2
>>DSx Flow Control	5.3.2.294	M	See IEEE802.16e for further details.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>Maximum MAC Data per Frame Support	5.3.2.296	M	See IEEE802.16e for further details.	1,2
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	M	See IEEE802.16e for further details.	1,2

TLV	Reference	M/O	Notes	Applicability
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	M	See IEEE802.16e for further details.	1,2
>>Packing Support	5.3.2.299	M	See IEEE802.16e for further details.	1,2
>>MAC ertPS Support	5.3.2.300	M	See IEEE802.16e for further details.	1,2
>>Maximum Number of Bursts Transmitted Concurrently to the MS	5.3.2.301	M	See IEEE802.16e for further details.	1,2
>>HO Supported	5.3.2.302	M	See IEEE802.16e for further details.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	M	See IEEE802.16e for further details.	1,2
>>Mobility Features Supported	5.3.2.304	M	See IEEE802.16e for further details.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	M	See IEEE802.16e for further details.	1,2
>>Idle Mode Timeout	5.3.2.268	M	See IEEE802.16e for further details.	1,2
>>ARQ Ack Type	5.3.2.307	M	See IEEE802.16e for further details.	1,2
>>MS HO Connections Parameters Proc Time	5.3.2.308	M	See IEEE802.16e for further details.	1,2
>>MS HO TEK Proc Time	5.3.2.309	M	See IEEE802.16e for further details.	1,2
>>MAC Header and Extended Sub-Header Support	5.3.2.310	M	See IEEE802.16e for further details.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	M	See IEEE802.16e for further details.	1,2
>>BS Switching Timer	5.3.2.314	M	See IEEE802.16e for further details.	1,2
>>Power Saving Class Capability	5.3.2.315	M	See IEEE802.16e for further details.	1,2
>>MAXIMUM_ARQ_ BUFFER_SIZE	5.3.2.532	O	See IEEE802.16m for further details.	3
>>MAXIMUM_NON_ ARQ_BUFFER_SIZE	5.3.2.533	O	See IEEE802.16m for further details.	3
>>Multicarrier capabilities	5.3.2.485	O	See IEEE802.16m for further details.	3
>>Zone Switch Mode	5.3.2.486	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
Support				
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O	See IEEE802.16m for further details.	3
>>Interference mitigation supported	5.3.2.488	O	See IEEE802.16m for further details.	3
>>E-MBS capabilities	5.3.2.489	O	See IEEE802.16m for further details.	3
>>Channel BW and Cyclic prefix	5.3.2.490	O	See IEEE802.16m for further details.	3
>>frame configuration to support legacy R1.0	5.3.2.491	O	See IEEE802.16m for further details.	3
>>Persistent Allocation support	5.3.2.492	O	See IEEE802.16m for further details.	3
>>Group Resource Allocation support	5.3.2.493	O	See IEEE802.16m for further details.	3
>>Co-located coexistence capability support	5.3.2.494	O	See IEEE802.16m for further details.	3
>>HO Trigger Metric Support	5.3.2.326	O	See IEEE802.16m for further details.	3
>>EBB Handover support	5.3.2.495	O	See IEEE802.16m for further details.	3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O	See IEEE802.16m for further details.	3
>>Capability for sounding antenna switching support	5.3.2.497	O	See IEEE802.16m for further details.	3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O	See IEEE802.16m for further details.	3
>>ROHC support	5.3.2.499	O	See IEEE802.16m for further details.	3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O	See IEEE802.16m for further details.	3
>Authenticator ID	5.3.2.19	M	Anchor Authenticator of the MS/AMS.	1,2,3
>SF Info	5.3.2.185	M		1,2,3
>>SFID	5.3.2.184	M		1,2,3
>>SF Type	5.3.2.306	O		1,2,3
>>Direction	5.3.2.59	M		1,2,3

TLV	Reference	M/O	Notes	Applicability
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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.	1,2
>>CS Type	5.3.2.39	O	This TLV must be included in the transmitted message for the target ASN to setup flow.	1,2,3
>>ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.	1,2,3
>>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.	1,2,3
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1,2,3
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_SYNC_LOSS_TIMEOUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted	1,2,3

TLV	Reference	M/O	Notes	Applicability
			message.	
>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>SN Feedback Enabled field	5.3.2.468	O		1,2
>>FSN Size	5.3.2.469	O		1,2
>>>ARQ_SUB_BLOCK_SIZE	5.3.2.531	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_ERROR_DETECTION_TIMEOUT	5.3.2.534	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_FEEDBACK_POLL_RETRY_TIMEOUT	5.3.2.535	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>CID	5.3.2.29	O		1,2
>>FID	5.3.2.471	O		3
>>SAID	5.3.2.169	O		1,2,3
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O		1,2,3
>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule.	1,2,3
>>>Classification Rule Priority	5.3.2.32	CM		1,2,3
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...	1,2,3
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.	1,2,3
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.	1,2,3

TLV	Reference	M/O	Notes	Applicability
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.	1,2,3
>>>IPv6 Flow Label	5.3.2.470	O		1,2,3
>>QoS Parameters	5.3.2.141	M		1,2,3
>>> DSCP	5.3.2.409	O	TC bit set to 1	1,2,3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1,2,3
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmiss	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3

TLV	Reference	M/O	Notes	Applicability
ion Policy				
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmiss	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3

TLV	Reference	M/O	Notes	Applicability
ion Policy				
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1,2,3
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1,2,3
>>>Media Flow Type	5.3.2.94	O		1,2,3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1,2,3
>>>Reduced Resources Code	5.3.2.237	O		1,2,3
>>PHS Rule	5.3.2.127	O		1,2,3
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSF	0	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
> Anchor ASN GW ID	5.3.2.10	M	Anchor DPF/FA of the MS/AMS.	1,2,3
> 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.	1,2,3
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted	1,2

TLV	Reference	M/O	Notes	Applicability
			message.	
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>Mobility Access Classifier	5.3.2.423	O	Shall be included by the BS/ABS if the MS mobility access classifier is fixed or nomadic and the BS/ABS supports Mobility Restriction for stationary access.	1,2,3
>Reattachment-Zone	5.3.2.424	O	Shall be included by the BS/ABS if the MS mobility access classifier is included.	1,2,3
Paging Information	5.3.2.119	M		1,2,3
> current Paging Cycle	5.3.2.481	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3

TLV	Reference	M/O	Notes	Applicability
> current Paging Offset	5.3.2.482	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
> current Deregistration ID	5.3.2.483	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
>current Paging Group ID	5.3.2.484	M	Parameter which was assigned to AMS by anchor PC as obtained from the AAI-RNG-REQ message.	3
>IDLE Mode Retain Info	5.3.2.81	M	IDLE Mode Retain Info.	1,2,3
Refresh IP address trigger	5.3.2.375	O	Included for the BS/ABS to trigger IP address refresh on the MS/AMS via HO Process Optimization TLV Bit #13. Currently used only for Simple IP re-anchoring.	1,2,3

Table 4-180 – IM_Exit_State_Ind

TLV	Description	M/O	Notes	Applicability
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS/ABS performing operation.	1,2,3
MS Info	5.3.2.103	M		1,2,3
> CMAC_Key_Count	5.3.2.34	M		1,2,3
> Authenticator ID	5.3.2.19	M		1,2,3
Idle Mode Exit Indicator	5.3.2.369	M	The values are: • 0 = Idle Mode Exit. • 1 = MS/AMS in Idle Mode.	1,2,3

Table 4-181 – IM_Exit_State_Ind_Ack

TLV	Reference	M/O	Notes	Applicability
BS Info	5.3.2.26	O		1,2,3
>BS ID	5.3.2.25	CM		1,2,3
Failure Indication	5.3.2.69	O		1,2,3

Table 4-182 – Path_Reg_Ack over R4

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS/ABS performing operation.	1,2,3
> Serving/Target Indicator	5.3.2.182	M	Set to “Serving”.	1,2,3

Table 4-183 – Context Req over R4

TLV	Reference	M/O	Notes	Applicability
Context Purpose Indicator	5.3.2.36	M	Bitmap indicating the required context. Set to indicate the AK Context.	1,2,3
BS Info (Serving)	5.3.2.26	M		1,2,3
> BS ID	5.3.2.25	M	The BSID received in the R4 IM_Exit_State_Change_Req.	1,2,3

Table 4-184 – Context Rpt over R4

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Provide failure indication for this message.	1,2,3
Context Purpose Indicator	5.3.2.36	M		1,2,3
MS Info	5.3.2.103	M		3
>CRID	5.3.2.475	M		3
BS Info (Serving)	5.3.2.26	M		1,2,3
> BS ID	5.3.2.25	M	BSID received in the corresponding R4 Context Request.	1,2,3
> AK Context	5.3.2.6	M		1,2,3
>>AK	5.3.2.5	M		1,2,3
>>AK ID	5.3.2.7	M		1,2,3
>>AK Lifetime	5.3.2.8	M		1,2,3
>>AK SN	5.3.2.9	M		1,2,3
>>CMAC_KEY_COUN	5.3.2.34	M		1,2,3

TLV	Reference	M/O	Notes	Applicabilit y
T				

4.10.5 Idle Mode Entry

Both MS/AMS and the network may initiate the procedure of entering Idle Mode.

In case that MS/AMS would enter idle mode at the BS or LZone of ABS, the PC assigns the MS/AMS paging information such as the tuple of Paging Group ID, Paging Cycle, Paging Offset.

But, in case that AMS would enter idle mode at the MZone of ABS, the PC assigns AMS the paging information such as the tuple of Paging Group ID, Paging Cycle, Paging Offset and Deregistration ID, which identifies uniquely the AMS in idle mode operation.

4.10.5.1 MS Initiated Idle Mode Entry

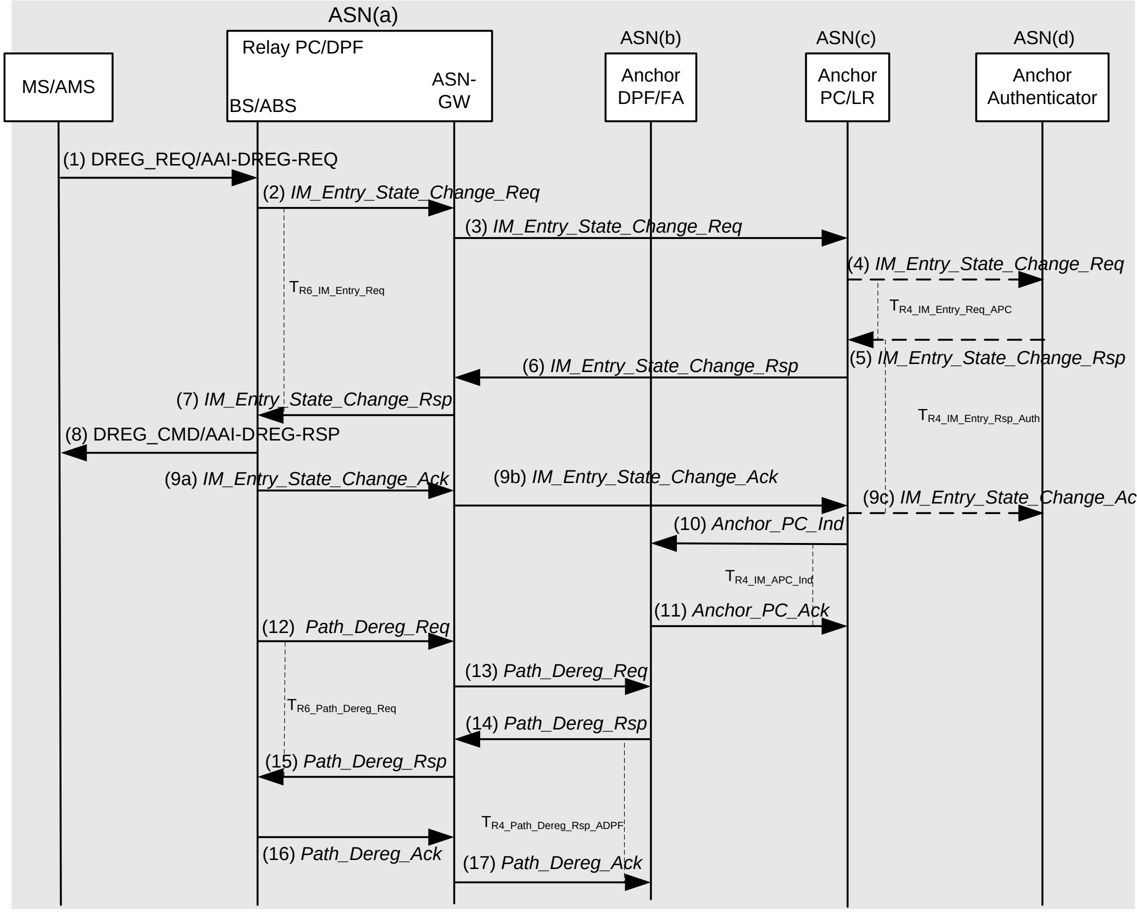


Figure 4-181 – MS Initiated Idle Mode Entry

STEP 1

MS/AMS decides to enter Idle Mode and sends DREG_REQ/AAI-DREG-REQ formatted as described in IEEE 802.16e/m. The De-Registration Request code is set to 0x01 indicating that the MS/AMS intends to enter Idle Mode.

STEP 2

Based on the MS/AMS's request, the BS/ABS(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/ABS(PA).

STEP 3

The local Relay PC in ASN(a) chooses an Anchor PC for the MS/AMS 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/AMS 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/AMS 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/AMS entering Idle Mode is sent successfully, Anchor Authenticator stores Anchor PC ID for this MS/AMS. 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/AMS 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/ABS(PA) including accepted Paging parameters. Upon reception of this message at the BS/ABS, timer $T_{R6\_IM\_Entry\_Req}$ is stopped.

STEP 8

BS/ABS sends DREG_CMD/AAI-DREG-RSP to the MS/AMS as specified in IEEE 802.16e/m. The DREG-CMD/AAI-DREG-RSP conveys "PC ID" field pointing to Anchor PC for the MS/AMS and allocated Idle mode parameters (i.e. DREG-CMD includes PGID, Paging Cycle, Paging offset and Paging listening interval. AAI-DREG-RSP includes PG ID, Paging Cycle, Paging offset and Deregistration ID).

STEP 9

9a: After sending the DREG_CMD/AAI-DREG-RSP to the MS/AMS, the BS/ABS(PA) acknowledges the successful delivery of DREG_CMD/AAI-DREG-RSP 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/AMS 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/AMS into LR database and SHALL send Anchor PC Indication message to ASN(b) associated with Anchor DPF/FA to reflect the success of MS/AMS 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/AMS including the Anchor PC ID of this MS/AMS 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/m parameter), BS/ABS 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/ABS starts timer $T_{R6\_Path\_Dreg\_Req}$ 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/AMS 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/ABS(PA) as R6 Path Dereg Response. Upon reception of this message $T_{R6\_Path\_Dreg\_Req}$ is stopped.

STEP 16

The BS/ABS(PA) completes the Data Path Dereg process for this MS/AMS 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

4.10.5.2.1 Idle Mode Entry in BS or LZone of ABS

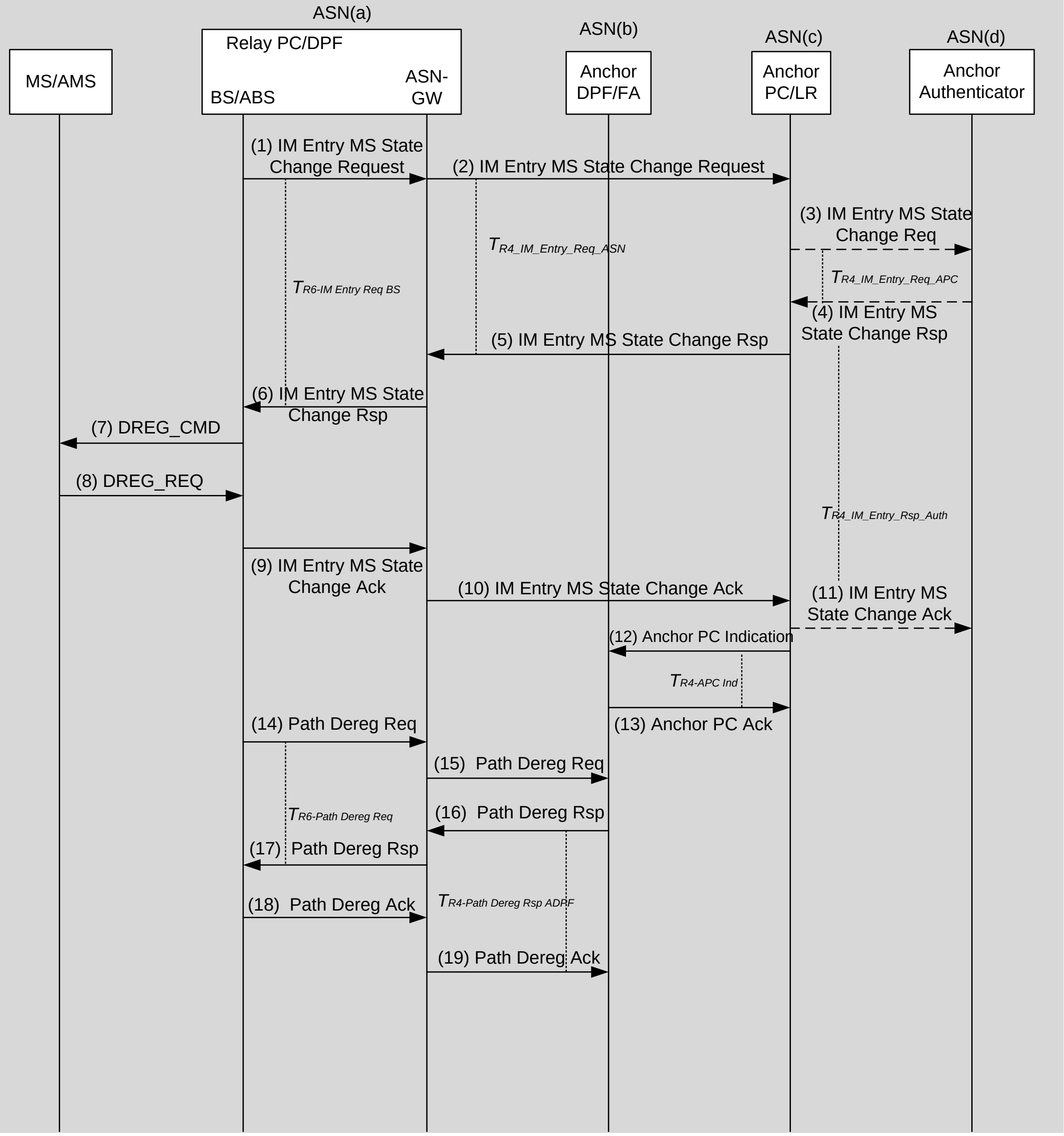

ASN(a)
Relay PC/DPF
BS/ABS
ASN-GW
MS/AMS
ASN(b)
Anchor DPF/FA
ASN(c)
Anchor PC/LR
ASN(d)
Anchor Authenticator
(1) IM Entry MS State Change Request
(2) IM Entry MS State Change Request
(3) IM Entry MS State Change Req
$T_{R4\_IM\_Entry\_Req\_ASN}$
$T_{R4\_IM\_Entry\_Req\_APC}$
$T_{R6\text{-}IM\ Entry\ Req\ BS}$
(4) IM Entry MS State Change Rsp
(5) IM Entry MS State Change Rsp
(6) IM Entry MS State Change Rsp
(7) DREG_CMD
(8) DREG_REQ
$T_{R4\_IM\_Entry\_Rsp\_Auth}$
(9) IM Entry MS State Change Ack
(10) IM Entry MS State Change Ack
(11) IM Entry MS State Change Ack
(12) Anchor PC Indication
$T_{R4\text{-}APC\ Ind}$
(13) Anchor PC Ack
(14) Path Dereg Req
(15) Path Dereg Req
$T_{R6\text{-}Path\ Dereg\ Req}$
(16) Path Dereg Rsp
(17) Path Dereg Rsp
(18) Path Dereg Ack
$T_{R4\text{-}Path\ Dereg\ Rsp\ ADPF}$
(19) Path Dereg Ack

Figure 4-182 – Network Initiated Idle Mode Entry in BS or LZone of ABS

Network may also initiate the MS/AMS 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/ABS(PA) decides to trigger MS/AMS 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/ABS(PA) to monitor the response message.

STEP 2

The Relay PC in ASN(a) associated with the Serving BS/ABS (PA) will check the received message and recommend an Anchor PC and paging information for the MS/AMS. 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/AMS 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/AMS location information (BSID, Relay PC ID, PGID etc) and other parameters, and send R4 *IM_Entry_State_Change_Req* message to the MS/AMS's Anchor authenticator to verify whether the MS/AMS 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/AMS 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/ABS(PA). When the serving BS/ABS(PA) receives this message it stops the timer $T_{R6\_IM\_Entry\_Req}$.

STEP 7

The serving BS/ABS(PA) sends DREG-CMD with Action Code TLV set to 0x05 to the MS/AMS 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/AMS as well as other paging parameters for the MS/AMS operation in Idle mode. The REQ-duration TLV may be included to indicate to the MS/AMS when to go to into Idle Mode. If the REQ-duration TLV is not included in the message, the Serving BS/ABS sets Timer $T_{46.}$

STEP 8

MS/AMS sends DREG-REQ to the BS/ABS(PA) as specified in IEEE 802.16e., acknowledging the Idle mode entry. . If the *REQ-duration* TLV was not sent to the MS/AMS, the MS/AMS 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/AMS, the MS/AMS 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/ABS sends a new DREG-CMD message with Action Code TLV set to 0x05.

STEP 9

Upon reception of DREG_REQ from MS/AMS, the BS/ABS(PA) sends R6 *IM_Entry_State_Change_Ack* to Relay PC in ASN(a) to notify that the MS/AMS 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/AMS 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/AMS 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/AMS 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/AMS including the Anchor PC ID of this MS/AMS 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/ABS 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/ABS starts timer $T_{R6\_Path\_Dreg\_Req}$ 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/AMS and gives the response the message R4 Path Dereg Response to ASN(a).

ASN(a) forwards the message to the BS/ABS as R6 Path Dereg Response. Upon reception of this message $T_{R6\text{-}Path\ Dereg\ Req}$ is stopped.

STEP 17

The BS/ABS completes the Data Path Dereg process for this MS/AMS 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 $T_{R4\_Path\_Dreg\_Rsp\_ADPF.}$

4.10.5.2.2 Idle Mode Entry in MZone of ABS

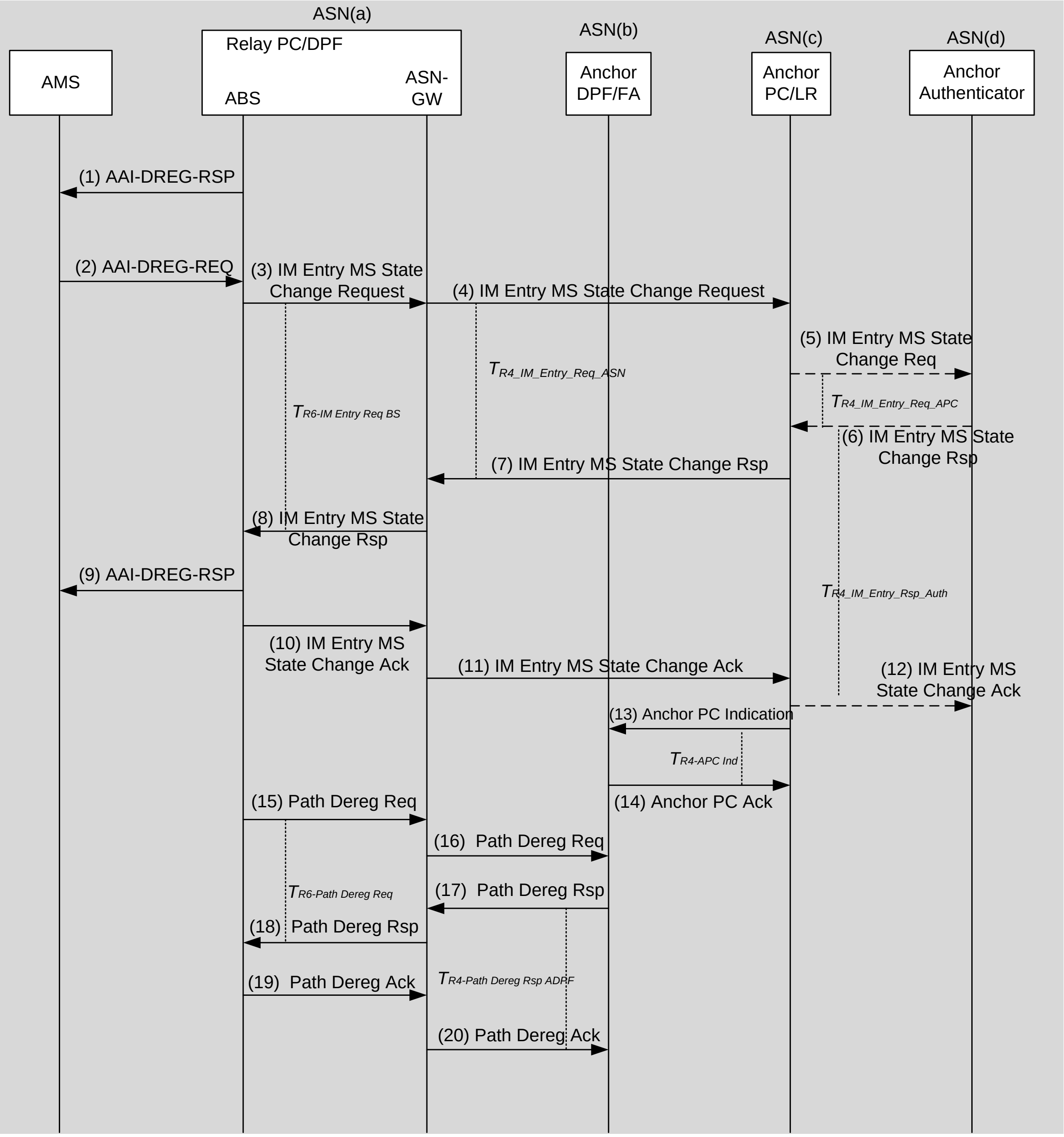

ASN(a)
Relay PC/DPF
AMS
ABS
ASN-GW
ASN(b)
Anchor DPF/FA
ASN(c)
Anchor PC/LR
ASN(d)
Anchor Authenticator
(1) AAI-DREG-RSP
(2) AAI-DREG-REQ
(3) IM Entry MS State Change Request
(4) IM Entry MS State Change Request
(5) IM Entry MS State Change Req
$T_{R4\_IM\_Entry\_Req\_ASN}$
$T_{R4\_IM\_Entry\_Req\_APC}$
$T_{R6\text{-}IM\ Entry\ Req\ BS}$
(6) IM Entry MS State Change Rsp
(7) IM Entry MS State Change Rsp
(8) IM Entry MS State Change Rsp
(9) AAI-DREG-RSP
$T_{R4\_IM\_Entry\_Rsp\_Auth}$
(10) IM Entry MS State Change Ack
(11) IM Entry MS State Change Ack
(12) IM Entry MS State Change Ack
(13) Anchor PC Indication
$T_{R4\text{-}APC\ Ind}$
(15) Path Dereg Req
(14) Anchor PC Ack
(16) Path Dereg Req
$T_{R6\text{-}Path\ Dereg\ Req}$
(17) Path Dereg Rsp
(18) Path Dereg Rsp
(19) Path Dereg Ack
$T_{R4\text{-}Path\ Dereg\ Rsp\ ADPF}$
(20) Path Dereg Ack

Figure 4-183 – Network Initiated Idle Mode Entry in MZone of ABS

Network may also initiate the AMS 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 ABS(PA) decides to trigger AMS entering Idle Mode and sends AAI-DREG-RSP with Action Code set to 0x05, which SHALL include REQ-duration timer, to the AMS as specified in IEEE 802.16m, asking it to enter

Idle mode. The “PC ID” field in AAI-DREG-RSP will contain the Anchor PC for the AMS as well as other paging parameters for the AMS operation in Idle mode.

STEP 2

AMS sends AAI-DREG-REQ to the ABS(PA) as specified in IEEE 802.16m. The AMS responds with the AAI-DREG-REQ message after expiration of the *REQ-duration* timer with *De-Registration_Request_Code* set to 0x01.

STEP 3

Based on the AMS’s request, the ABS(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 ABS(PA).

STEP 4

The local Relay PC in ASN(a) chooses an Anchor PC for the AMS and sends inter-ASN R4 *IM_Entry_State_Change_Req* message to the ASN(c) associated with the chosen Anchor PC.

STEP 5

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 AMS 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 6

ASN(d) associated with Anchor Authenticator checks if the AMS 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 AMS entering Idle Mode is sent successfully, Anchor Authenticator stores Anchor PC ID for this AMS. 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 7

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 AMS location information (PGID) and other parameters, and sends back R4 *IM_Entry_State_Change_Rsp* message to ASN(a).

STEP 8

ASN(a) forwards the R6 *IM_Entry_State_Change_Rsp* to serving ABS(PA) including accepted Paging parameters. Upon reception of this message at the ABS, timer $T_{R6\_IM\_Entry\_Req}$ is stopped.

STEP 9

ABS sends AAI-DREG-RSP with Action Code set to 0x07 to the AMS as specified in IEEE 802.16m. The AAI-DREG-RSP conveys “PC ID” field pointing to Anchor PC for the AMS and allocated Idle mode parameters (PGID, Paging Cycle, Paging offset and Deregistration ID).

STEP 10

After sending the AAI-DREG-RSP to the AMS, the ABS(PA) acknowledges the successful delivery of AAI-DREG-RSP to the local Relay PC in ASN(a) by sending R6 *IM_Entry_State_Change_Ack*.

STEP 11

The local Relay PC in ASN(a) forwards the successful entry of AMS 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.

STEP 12

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 13

ASN(c) associated with Anchor PC/LR updates the information of AMS into LR database and SHALL send Anchor PC Indication message to ASN(b) associated with Anchor DPF/FA to reflect the success of AMS entering Idle Mode. Timer $T_{R4\_APC\_Ind}$ is started at this time when Anchor PC Indication is sent to monitor the response.

STEP 14

The ASN(b) associated with Anchor DPF/FA finally updates the information of AMS including the Anchor PC ID of this AMS 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 15

After the expiration of the Management Resource Holding Timer (an 802.16m parameter), ABS 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 ABS starts timer $T_{R6\_Path\_Dreg\_Req}$ to monitor the response.

STEP 16

ASN-GW in ASN(a) forwards the message as R4 Path Dereg Req to the ASN(b) associated with the Anchor DPF/FA.

STEP 17

ASN(b) completes the Path deregistration process for this AMS and gives the response the message R4 Path Dereg Response to ASN(a).

STEP 18

ASN-GW in ASN(a) forwards the message to the ABS(PA) as R6 Path Dereg Response. Upon reception of this message $T_{R6\_Path\_Dreg\_Req}$ is stopped.

STEP 19

The ABS(PA) completes the Data Path Dereg process for this AMS and acknowledges it by sending R6 *Path_Dereg_Ack* to the ASN(a).

STEP 20

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 $T_{Path\_Dereg\_Rsp\_ADPF.}$

4.10.5.3 Idle Mode Entry Timers and Timing Considerations:

This section defines the timer entities defined for the Idle Mode entry procedure.

- $T_{\text{R6\_IM\_Entry\_Req}}$: Started by the Serving BS/ABS 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.
- $T_{\text{R4\_IM\_Entry\_Req\_ASN}}$: 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.
- $T_{\text{R4\_IM\_Entry\_Req\_APC}}$: 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*.
- $T_{\text{R4 IM Entry Rsp Auth}}$: 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.
- $T_{\text{R4\_APC\_Ind}}$: 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.
- $T_{\text{R6\_Path\_Dreg\_Req:}}$ Started by the Serving BS/ABS 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.
- $T_{\text{R4\_Path\_Dreg\_Rsp\_ADPF:}}$ 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/LZone of ABS after sending a DREG-CMD message to the MS/AMS for network initiated Idle Mode. The T_{46} timer is not set if the MS/AMS is instructed to enter Idle Mode at a later time.

Table 4-185 shows the default value of timers and also indicates the range of the recommended duration of these timers.

Table 4-185 – Idle Mode Entry Timer Values

Timer	Default Values (msec)	Criteria	Maximum Value
$T_{\text{R6\_IM\_Entry\_Req}}$	TBD		TBD
$T_{\text{R4\_IM\_Entry\_Req\_APC}}$	TBD		TBD
$T_{\text{R4\_APC\_Ind}}$	TBD		TBD
$T_{\text{R6\_Path\_Dreg\_Req}}$	TBD		TBD
$T_{\text{R4\_Path\_Dreg\_Rsp\_ADPF}}$	TBD		TBD
T_{46}	TBD		TBD
$T_{\text{R4\_IM\_Entry\_Req\_ASN}}$	TBD		TBD
$T_{\text{ R4 IM Entry Rsp Auth}}$	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 4-186 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 4-186.

Table 4-186 – Timer Max Retry Conditions

Timer	Entity where Timer Started	Action(s)
$T_{R6\_IM\_Entry\_Req}$	BS/ABS(PA)	Idle mode entry procedure is not progressing hence procedure is terminated, MS/AMS allowed to be Active. If initiated by MS/AMS, DREG_CMD/AAI-DREG-RSP with appropriate action code for either 'continue normal operation' or try after a time out is send out. If network initiated, the BS/ABS continues with the normal operation of the MS/AMS allowing the MS/AMS to be active.
$T_{R4\_IM\_Entry\_Req\_APC}$	Anchor PC	No Action Required.
$T_{R4\_APC\_Ind}$	Anchor PC	Sends R4 *IM_Entry_State_Change_Req* to Anchor Authenticator to revert back the MS state to active. All actions taken at Anchor PC to change the state of MS/AMS is cancelled. MS/AMS allowed to be Active.
$T_{R4\_IM\_Entry\_Rsp\_Auth}$		Failure indication sent downstream to the Anchor PC/LR.
$T_{R6\_Path\_Dreg\_Req}$		The BS will perform error handling as per local policy.
$T_{R4\_Path\_Dreg\_Rsp\_ADPF}$		The Anchor DPF will perform error handling as per local policy.
$T_{R4\_IM\_Entry\_Req\_ASN}$	Serving ASN	No Action Required.
T_{46}	BS/ABS	BS/ABS stops sending DREG-CMD/AAI-DREG-RSP to MS/AMS. 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/AMS is allowed to go idle and it is possible for network to support the MS/AMS 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/ABS 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/ABS. The serving BS/ABS 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 4-187 – IM_Entry_State_Change_Req over R6

TLV	Reference	M/O	Notes	Applicabilit y
BS Info	5.3.2.26	M		1,2,3
> BS ID	5.3.2.25	M	BS ID indicating the Serving BS/ABS performing operation.	1,2,3
MS Info	5.3.2.103	M		1,2,3
>CRID	5.3.2.475	M		3
>Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS/AMS. 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/AMS 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.	1,2,3
>>CS Type	5.3.2.39	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1,2,3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1,2,3
>SBC Context	5.3.2.174	M		1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>HARQ Enable (one or more)	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.	1,2
>>>Direction	5.3.2.59	O	Indicates the direction of the management connection.	1,2
>>>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	1,2

TLV	Reference	M/O	Notes	Applicability
			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.	1,2
>>Subscriber Transition Gaps	5.3.2.316	M	See IEEE802.16e for further details.	1,2
>>Maximum Transmit Power	5.3.2.317	M	See IEEE802.16e/m for further details.	1,2,3
>>Capabilities for Construction and Transmission of MAC PDUs	5.3.2.318	M	See IEEE802.16e for further details.	1,2
>>PKM Flow Control	5.3.2.319	M	See IEEE802.16e for further details.	1,2
>>Maximum Number of Supported Security Associations	5.3.2.320	M	See IEEE802.16e for further details.	1,2
>>Security Negotiation Parameters	5.3.2.321	M	See IEEE802.16e/m for further details.	1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2,3
>>>Authorization Policy Support	5.3.2.21	M	See IEEE802.16e/m for further details.	1,2,3
>>>MAC Mode	5.3.2.322	M	See IEEE802.16e for further details.	1,2
>>>PN Window Size	5.3.2.324	M	See IEEE802.16e/m for further details.	1,2,3
>>Association type support	5.3.2.465	O		1,2
>>>Size of ICV	5.3.2.502	M	See IEEE802.16m for further details.	3
>>Extended Subheader Capability	5.3.2.325	M	See IEEE802.16e for further details.	1,2
>>HO Trigger Metric Support	5.3.2.326	M	See IEEE802.16e for further details.	1,2
>>Current Transmit Power	5.3.2.327	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	M	See IEEE802.16e/m for further details.	1,2,3
>>OFDMA SS demodulator	5.3.2.329	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS	5.3.2.330	M	See IEEE802.16e for further details.	1,2

TLV	Reference	M/O	Notes	Applicability
modulator				
>>The number of UL HARQ Channel	5.3.2.331	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Permutation support	5.3.2.332	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS CINR Measurement Capability	5.3.2.333	M	See IEEE802.16e for further details.	1,2
>>The number of DL HARQ Channels	5.3.2.334	M	See IEEE802.16e for further details.	1,2
>>HARQ Chase Combining and CC-IR Buffer Capability	5.3.2.335	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Uplink Power Control Support	5.3.2.336	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS Uplink Power Control Scheme Switching Delay	5.3.2.337	M	See IEEE802.16e for further details.	1,2
>>OFDMA MAP Capability	5.3.2.338	M	See IEEE802.16e for further details.	1,2
>>Uplink Control Channel Support	5.3.2.339	M	See IEEE802.16e for further details.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	M	See IEEE802.16e for further details.	1,2
>>Maximum Number of Burst per Frame Capability in HARQ	5.3.2.341	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS demodulator for MIMO Support	5.3.2.342	M	See IEEE802.16e for further details.	1,2
>>OFDMA SS modulator for MIMO Support	5.3.2.343	M	See IEEE802.16e for further details.	1,2
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	M	See IEEE802.16e for further details.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O	See IEEE802.16m for further details.	3
>>DEVICE_CLASS	5.3.2.504	O	See IEEE802.16m for further details.	3
>>CLC Request	5.3.2.505	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
>>Long TTI for DL	5.3.2.506	O	See IEEE802.16m for further details.	3
>>UL sounding	5.3.2.507	O	See IEEE802.16m for further details.	3
>>OL Region	5.3.2.508	O	See IEEE802.16m for further details.	3
>>DL resource metric for FFR	5.3.2.509	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O	See IEEE802.16m for further details.	3
>>DL MIMO mode	5.3.2.512	O	See IEEE802.16m for further details.	3
>>feedback support for DL	5.3.2.513	O	See IEEE802.16m for further details.	3
>>Subband assignment A-MAP IE support	5.3.2.514	O	See IEEE802.16m for further details.	3
>>DL pilot pattern for MU MIMO	5.3.2.515	O	See IEEE802.16m for further details.	3
>>Number of Tx antenna of AMS	5.3.2.516	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O	See IEEE802.16m for further details.	3
>>UL pilot pattern for MU MIMO	5.3.2.519	O	See IEEE802.16m for further details.	3
>>UL MIMO mode	5.3.2.520	O	See IEEE802.16m for further details.	3
>>Modulation scheme	5.3.2.521	O	See IEEE802.16m for further details.	3
>>UL HARQ buffering capability	5.3.2.522	O	See IEEE802.16m for further details.	3
>>DL HARQ buffering capability	5.3.2.523	O	See IEEE802.16m for further details.	3
>>AMS DL processing capability per sub-frame	5.3.2.524	O	See IEEE802.16m for further details.	3
>>AMS UL processing capability per sub-frame	5.3.2.525	O	See IEEE802.16m for further details.	3
>>FFT size(2048/1024/512)	5.3.2.526	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
>>Authorization policy support	5.3.2.21	O	See IEEE802.16m for further details.	3
>>Inter-RAT Operation Mode	5.3.2.527	O	See IEEE802.16m for further details.	3
>>Supported Inter-RAT type	5.3.2.528	O	See IEEE802.16m for further details.	3
>>MIH Capability Supported	5.3.2.529	O	See IEEE802.16m for further details.	3
> REG context	5.3.2.144	M		1,2,3
>>Number of UL Transport CIDs Support	5.3.2.288	M	See IEEE802.16e for further details.	1,2
>>Number of DL Transport CIDs Support	5.3.2.289	M	See IEEE802.16e for further details.	1,2
>>Classification/PHS Options and SDU Encapsulation Support	5.3.2.290	M	See IEEE802.16e/m for further details. It is named as 'CS type support' in 16m.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	M	See IEEE802.16e/m for further details.	1,2,3
>>PHS Support	5.3.2.292	M	See IEEE802.16e/m for further details.	1,2,3
>>ARQ Support	5.3.2.293	M	See IEEE802.16e for further details. For 16m the value may be set by 1(i.e. ARQ is supported).	1,2
>>DSx Flow Control	5.3.2.294	M	See IEEE802.16e for further details.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>Maximum MAC Data per Frame Support	5.3.2.296	M	See IEEE802.16e for further details.	1,2
>>>Maximum amount of MAC Level Data per DL Frame	5.3.2.297	M	See IEEE802.16e for further details.	1,2
>>>Maximum amount of MAC Level Data per UL Frame	5.3.2.298	M	See IEEE802.16e for further details.	1,2
>>Packing Support	5.3.2.299	M	See IEEE802.16e for further details. For 16m the value may be set by 1(i.e. packing supported).	1,2
>>MAC ertPS Support	5.3.2.300	M	See IEEE802.16e for further details. For 16m the value may be set by 1(i.e. packing supported).	1,2
>>Maximum Number of	5.3.2.301	M	See IEEE802.16e for further details.	1,2

TLV	Reference	M/O	Notes	Applicability
Bursts Transmitted Concurrently to the MS				
>>HO Supported	5.3.2.302	M	See IEEE802.16e for further details.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	M	See IEEE802.16e for further details.	1,2
>>Mobility Features Supported	5.3.2.304	M	See IEEE802.16e for further details.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	M	See IEEE802.16e for further details.	1,2
>>Idle Mode Timeout	5.3.2.268	M	See IEEE802.16e for further details.	1,2
>>ARQ Ack Type	5.3.2.307	M	See IEEE802.16e for further details.	1,2
>>MS HO Connections Parameters Proc Time	5.3.2.308	M	See IEEE802.16e for further details.	1,2
>>MS HO TEK Proc Time	5.3.2.309	M	See IEEE802.16e for further details.	1,2
>>MAC Header and Extended Sub-Header Support	5.3.2.310	M	See IEEE802.16e for further details.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	M	See IEEE802.16e for further details.	1,2
>>BS Switching Timer	5.3.2.314	M	See IEEE802.16e for further details.	1,2
>>Power Saving Class Capability	5.3.2.315	M	See IEEE802.16e for further details.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O	See IEEE802.16m for further details.	3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O	See IEEE802.16m for further details.	3
>>Multicarrier capabilities	5.3.2.485	O	See IEEE802.16m for further details.	3
>>Zone Switch Mode Support	5.3.2.486	O	See IEEE802.16m for further details.	3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O	See IEEE802.16m for further details.	3
>>Interference mitigation supported	5.3.2.488	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicabilit y
>>E-MBS capabilities	5.3.2.489	O	See IEEE802.16m for further details.	3
>>Channel BW and Cyclic prefix	5.3.2.490	O	See IEEE802.16m for further details.	3
>>frame configuration to support legacy R1.0	5.3.2.491	O	See IEEE802.16m for further details.	3
>>Persistent Allocation support	5.3.2.492	O	See IEEE802.16m for further details.	3
>>Group Resource Allocation support	5.3.2.493	O	See IEEE802.16m for further details.	3
>>Co-located coexistence capability support	5.3.2.494	O	See IEEE802.16m for further details.	3
>>HO Trigger Metric Support	5.3.2.326	O	See IEEE802.16m for further details.	3
>>EBB Handover support	5.3.2.495	O	See IEEE802.16m for further details.	3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O	See IEEE802.16m for further details.	3
>>Capability for sounding antenna switching support	5.3.2.497	O	See IEEE802.16m for further details.	3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O	See IEEE802.16m for further details.	3
>>ROHC support	5.3.2.499	O	See IEEE802.16m for further details.	3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O	See IEEE802.16m for further details.	3
> 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.	1,2,3
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Older TEK	5.3.2.112	O	This TLV MAY be included if SA	1,2,

TLV	Reference	M/O	Notes	Applicabilit y
Parameters			Descriptor is included in the transmitted message.	
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2,
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2,
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2,
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2,
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2,
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2,
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2,
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2,
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2,
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2,
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2,
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>SF Info	5.3.2.185	M	Service Flow Information of the MS. Contains Service Flow information in the nested IEs.	1,2,3
>>SFID	5.3.2.184	M		1,2,3
>>SF Type	5.3.2.306	O		1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>HARQ Enable	5.3.2.454	O	Indicates support for HARQ on UL and	1,2

TLV	Reference	M/O	Notes	Applicability
			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.	1,2
>>>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.	1,2
>>Direction	5.3.2.59	M		1,2,3
>>CS Type	5.3.2.39	O	This TLV is included in the transmitted message for the target ASN to setup flow.	1,2,3
>> ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e.	1,2,3
>>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.	1,2,3
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1,2,3
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_SYNC_LOSS_TIMEOUT	5.3.2.350	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_BLOCK_SIZE	5.3.2.353	O	This TLV SHALL be included if ARQ Context is included in the transmitted	1,2

TLV	Reference	M/O	Notes	Applicabilit y
			message.	
>>>RECEIVER_ARQ_ ACK_PROCESSING TIME.	5.3.2.354	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>SN Feedback Enabled field	5.3.2.468	O		1,2
>>FSN Size	5.3.2.469	O		1,2
>>>ARQ_SUB_BLOC K_SIZE	5.3.2.531	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_ERROR_DE TECTION_TIMEOUT	5.3.2.534	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_FEEDBACK _POLL_RETRY_TIME OUT	5.3.2.535	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>CID	5.3.2.29	O		1,2
>>FID	5.3.2.471	O		3
>>SAID	5.3.2.169	O		1,2,3
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O		1,2,3
>>>Classification Rule Index	5.3.2.30	O	Index assigned to the Packet Classification Rule.	1,2,3
>>> Classification Rule Priority	5.3.2.32	O		1,2,3
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...	1,2,3
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.	1,2,3
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.	1,2,3
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.	1,2,3
>>>IPv6 Flow Label	5.3.2.470	O		1,2,3

TLV	Reference	M/O	Notes	Applicability
>>QoS Parameters	5.3.2.141	M		1,2,3
>>> DSCP	5.3.2.409	O	TC bit set to 1	1,2,3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1,2,3
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3

TLV	Reference	M/O	Notes	Applicability
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1,2,3

TLV	Reference	M/O	Notes	Applicability
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1,2,3
>>>Media Flow Type	5.3.2.94	O		1,2,3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1,2,3
>>>Reduced Resources Code	5.3.2.237	O		1,2,3
>>PHS Rule	5.3.2.127	O		1,2,3
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSF	0	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
> Authenticator ID	5.3.2.19	M	ID of Anchor Authenticator.	1,2,3
> Anchor ASN GW ID	5.3.2.10	M	ID of Anchor GW / Anchor DPF.	1,2,3
>Mobility Access Classifier	5.3.2.423	O	Shall be included by the BS/ABS if the MS mobility access classifier is fixed or nomadic and the BS/ABS supports Mobility Restriction for stationary access.	1,2,3
>Reattachment-Zone	5.3.2.424	O	Shall be included by the BS/ABS if the MS mobility access classifier is included.	1,2,3
Paging Information	5.3.2.119	M	Included based on the Paging Cycle TLV received from MS/AMS or if cached by the BS/ABS(PA). If not cached in the BS/ABS(PA), the BS/ABS(PA) will set the Page Group ID part of the TLV and may include the suggested values for Paging cycle and Offset.	1,2,3
> Paging Cycle	5.3.2.118	O	Included based on the Paging Cycle Request TLV received from MS/AMS or if cached by the BS/ABS.	1,2,3
> Paging Offset	5.3.2.120	O		1,2,3

TLV	Reference	M/O	Notes	Applicability
> Paging Interval Length	5.3.2.135	O		1,2
> Paging Group ID	5.3.2.123	O		1,2,3
> Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS/AMS, to be stored in Location Register.	1,2,3
> Idle Mode Retain Info	5.3.2.81	M	Included based on the bits set in the Idle mode retain information TLV from the MS/AMS or if cached by the BS/ABS.	1,2,3

Table 4-188 –Anchor_PC_Ind

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Included if idle mode entry is not successful.	1,2,3
Paging Information	5.3.2.119	M	Included if Failure Indication is not included.	1,2,3
>Anchor PC ID	5.3.2.12	M	Confirmed Paging Controller ID for the MS/AMS entering Idle mode.	1,2,3

Table 4-189 –Anchor_PC_Ack

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3

Table 4-190 – IM_Entry_State_Change_Req over R4

TLV	Reference	M/O	Notes	Applicability
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS/ABS performing operation.	1,2,3
MS Info	5.3.2.103	M		1,2,3
>CRID	5.3.2.475	M		3
>Combined Resource Indicator	5.3.2.206	O	This TLV indicates the Combined Resource Required flag is enabled or not for this MS/AMS. 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	1,2,3

TLV	Reference	M/O	Notes	Applicability
			are allowed for the MS/AMS 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.	1,2,3
>>Combined Resources Required	5.3.2.35	CM	This TLV SHALL be included if Combined Resource Indicator is included in the transmitted message.	1,2,3
>SBC Context	5.3.2.174	CM	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005.	1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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.	1,2
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>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.	1,2
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Number of Supported Security	5.3.2.320	CM	This TLV SHALL be included if SBC Context is included in the transmitted	1,2

TLV	Reference	M/O	Notes	Applicability
Associations			message.	
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>>PKM Version Support	5.3.2.464	O		1,2,3
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>MAC Mode	5.3.2.322	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>Association type support	5.3.2.465	O		1,2
>>>Size of ICV	5.3.2.502	M	See IEEE802.16m for further details.	3
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS CINR	5.3.2.333	CM	This TLV SHALL be included if SBC	1,2

TLV	Reference	M/O	Notes	Applicability
Measurement Capability			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.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA multiple DL burst profile capability	5.3.2.466	O		1,2
>>SDMA Pilot capability	5.3.2.467	O		1,2
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O	See IEEE802.16m for further details.	3
>>DEVICE_CLASS	5.3.2.504	O	See IEEE802.16m for further details.	3
>>CLC Request	5.3.2.505	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
>>Long TTI for DL	5.3.2.506	O	See IEEE802.16m for further details.	3
>>UL sounding	5.3.2.507	O	See IEEE802.16m for further details.	3
>>OL Region	5.3.2.508	O	See IEEE802.16m for further details.	3
>>DL resource metric for FFR	5.3.2.509	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O	See IEEE802.16m for further details.	3
>>DL MIMO mode	5.3.2.512	O	See IEEE802.16m for further details.	3
>>feedback support for DL	5.3.2.513	O	See IEEE802.16m for further details.	3
>>Subband assignment A-MAP IE support	5.3.2.514	O	See IEEE802.16m for further details.	3
>>DL pilot pattern for MU MIMO	5.3.2.515	O	See IEEE802.16m for further details.	3
>>Number of Tx antenna of AMS	5.3.2.516	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O	See IEEE802.16m for further details.	3
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O	See IEEE802.16m for further details.	3
>>UL pilot pattern for MU MIMO	5.3.2.519	O	See IEEE802.16m for further details.	3
>>UL MIMO mode	5.3.2.520	O	See IEEE802.16m for further details.	3
>>Modulation scheme	5.3.2.521	O	See IEEE802.16m for further details.	3
>>UL HARQ buffering capability	5.3.2.522	O	See IEEE802.16m for further details.	3
>>DL HARQ buffering capability	5.3.2.523	O	See IEEE802.16m for further details.	3
>>AMS DL processing capability per sub-frame	5.3.2.524	O	See IEEE802.16m for further details.	3
>>AMS UL processing capability per sub-frame	5.3.2.525	O	See IEEE802.16m for further details.	3
>>FFT size(2048/1024/512)	5.3.2.526	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
>>Authorization policy support	5.3.2.21	O	See IEEE802.16m for further details.	3
>>Inter-RAT Operation Mode	5.3.2.527	O	See IEEE802.16m for further details.	3
>>Supported Inter-RAT type	5.3.2.528	O	See IEEE802.16m for further details.	3
>>MIH Capability Supported	5.3.2.529	O	See IEEE802.16m for further details.	3
>REG context	5.3.2.144	CM	Included based on the bits set in the Idle mode retain information TLV from the MS. See IEEE802.16e-2005.	1,2,3
>>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.	1,2
>>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.	1,2
>>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.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAC flow control	5.3.2.462	O		1,2
>>Multicast polling group CID support	5.3.2.463	O		1,2
>>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.	1,2
>>>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.	1,2
>>>Maximum amount of MAC Level Data per	5.3.2.298	CM	This TLV SHALL be included if Maximum MAC Data per Frame Support	1,2

TLV	Reference	M/O	Notes	Applicability
UL Frame			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.	1,2
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted	1,2

TLV	Reference	M/O	Notes	Applicability
			message.	
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O	See IEEE802.16m for further details.	3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O	See IEEE802.16m for further details.	3
>>Multicarrier capabilities	5.3.2.485	O	See IEEE802.16m for further details.	3
>>Zone Switch Mode Support	5.3.2.486	O	See IEEE802.16m for further details.	3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O	See IEEE802.16m for further details.	3
>>Interference mitigation supported	5.3.2.488	O	See IEEE802.16m for further details.	3
>>E-MBS capabilities	5.3.2.489	O	See IEEE802.16m for further details.	3
>>Channel BW and Cyclic prefix	5.3.2.490	O	See IEEE802.16m for further details.	3
>>frame configuration to support legacy R1.0	5.3.2.491	O	See IEEE802.16m for further details.	3
>>Persistent Allocation support	5.3.2.492	O	See IEEE802.16m for further details.	3
>>Group Resource Allocation support	5.3.2.493	O	See IEEE802.16m for further details.	3
>>Co-located coexistence capability support	5.3.2.494	O	See IEEE802.16m for further details.	3
>>HO Trigger Metric Support	5.3.2.326	O	See IEEE802.16m for further details.	3
>>EBB Handover support	5.3.2.495	O	See IEEE802.16m for further details.	3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O	See IEEE802.16m for further details.	3
>>Capability for sounding antenna switching support	5.3.2.497	O	See IEEE802.16m for further details.	3

TLV	Reference	M/O	Notes	Applicability
>>Antenna configuration for sounding antenna switching	5.3.2.498	O	See IEEE802.16m for further details.	3
>>ROHC support	5.3.2.499	O	See IEEE802.16m for further details.	3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O	See IEEE802.16m for further details.	3
>Authenticator ID	5.3.2.19	M		1,2,3
>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.	1,2,3
>Reattachment-Zone	5.3.2.424	O	Shall be included if the MS mobility access classifier is included.	1,2,3
>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.	1,2,3
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older	1,2

TLV	Reference	M/O	Notes	Applicability
			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.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>SF Info	5.3.2.185	CM	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.	1,2,3
>> SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
>>SF Type	5.3.2.306	O		1,2,3
>> ARQ Enable	5.3.2.345	M	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e/m.	1,2,3
>>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.	1,2,3
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1,2,3
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2

TLV	Reference	M/O	Notes	Applicability
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_SYNC_LOSS_TIMEOUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_SUB_BLOCK_SIZE	5.3.2.531	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_ERROR_DETECTION_TIMEOUT	5.3.2.534	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>>ARQ_FEEDBACK_POLL_RETRY_TIMEOUT	5.3.2.535	O	This TLV SHALL be included if ARQ Context is included in the transmitted message.	3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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.	1,2
>>SN Feedback Enabled	5.3.2.468	O		1,2

TLV	Reference	M/O	Notes	Applicability
field				
>>FSN Size	5.3.2.469	O		1,2
>>Direction	5.3.2.59	M		1,2,3
>>CS Type	5.3.2.39	O	This TLV must be included in the transmitted message for the target ASN to setup flow.	1,2,3
>>SAID	5.3.2.169	O		1,2,3
>>QoS Parameters	5.3.2.141	M		1,2,3
>>> DSCP	5.3.2.409	O	TC bit set to 1	1,2,3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1,2,3
>>>>Minimum Reserved Traffic Rate	5.3.2.95	O	See IEEE802.16e for further details.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1,2,3
>>>>Minimum Reserved Traffic Rate	5.3.2.95	CM	This TLV SHALL be included if NRT-VR Data Delivery Service is included in the	1,2,3

TLV	Reference	M/O	Notes	Applicabilit y
			transmitted message.	
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in	1,2,3

TLV	Reference	M/O	Notes	Applicability
			milliseconds).	
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1,2,3
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1,2,3
>>>Media Flow Type	5.3.2.94	O		1,2,3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1,2,3
>>>Reduced Resources Code	5.3.2.237	O		1,2,3
>>PHS Rule	5.3.2.127	O		1,2,3
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSS	5.3.2.129	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSF	0	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
Paging Information	5.3.2.119	M	Paging Information TLV obtained from the BS/ABS containing PAGING_CYCLE, PAGING OFFSET, and Paging Group ID if present in R6 message.	1,2,3
> Paging Cycle	5.3.2.118	O		1,2,3
> Paging Offset	5.3.2.120	O		1,2,3
> Paging Interval Length	5.3.2.135	O		1,2,3
> Paging Group ID	5.3.2.123	O		1,2,3

TLV	Reference	M/O	Notes	Applicability
> Idle Mode Retain Info	5.3.2.81	M	Included based on the bits set in the Idle mode retain information TLV from the MS/AMS. See IEEE802.16e-2005. Optionally included in this R4 message if present in the corresponding R6 message.	1,2,3
>Relay PC ID	5.3.2.117	O	The Relay PC Identifier for the MS/AMS, to be stored in Location Register.	1,2,3
>Anchor PC ID	5.3.2.12	M	Recommended Anchor PC ID by the Relay PC.	1,2,3
>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.	1,2,3

Note: SBC Context, REG Context, SA Descriptor and SF Info. are only transmitted by Relay PC to Anchor PC.

Table 4-191 – IM_Entry_State_Change_Rsp

TLV	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Optional TLV if there is a failure.	1,2,3
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS/ABS performing operation. (To indicate destination BS/ABS for a relayed message, this IE is needed).	1,2,3
Paging Information	5.3.2.119	M	Paging Information TLV meant for the DREG-CMD/AAI-DREG-RSP to the MS/AMS containing PAGING_CYCLE, PAGING OFFSET, PAGING_INTERVAL_LENGTH, Deregistration ID 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.	1,2,3
>Anchor PC ID	5.3.2.12	O	Included if Paging Controller ID different than the APC received in R4 *IM_Entry_State_Change_Req* message.	1,2,3
> Paging Cycle	5.3.2.118	O	Included if different than that received in R4 *IM_Entry_State_Change_Req*. This TLV SHALL be included for IM entry in MZone of ABS.	1,2,3
> Paging Offset	5.3.2.120	O	Included if different than that received in R4 *IM_Entry_State_Change_Req*. This TLV SHALL be included for IM	1,2,3

TLV	Reference	M/O	Notes	Applicability
			entry in MZone of ABS.	
> Paging Interval Length	5.3.2.135	O	Included if different than that received in R4 *IM_Entry_State_Change_Req*. This TLV is available for IM entry in BS or LZone of ABS.	1,2
>Deregistration ID	5.3.2.480	M	This TLV SHALL be included for IM entry in MZone of ABS.	3
> Paging Group ID	5.3.2.123	O	This TLV SHALL be included if Paging Information is included in the transmitted message.	1,2,3
> 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 *IM_Entry_State_Change_Req*.	1,2,3
> Idle Mode Timeout	5.3.2.268	M	The Anchor PC/LR SHALL include to minimize Timeout mismatch between the system and devices.	1,2,3
MS Info	5.3.2.103	O		1,2,3
>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.	1,2,3
>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.	1,2,3

1 **Table 4-192 – IM_Entry_State_Change_Ack**

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O	Optional TLV if there is a failure by rejection of MS. Code Value = 52	1,2,3
BS Info	5.3.2.26	M		1,2,3
>BS ID	5.3.2.25	M	BS ID indicating the Serving BS/ABS performing operation.	1,2,3
Paging Information	5.3.2.119	M		1,2,3
>Anchor PC ID	5.3.2.12	M	Paging Controller ID Acting as Anchor PC.	1,2,3

2 ### 4.10.6 Idle Mode Operation and CSN Anchored Mobility Management

3 Support for Foreign Agent migration in Idle Mode is optional. FA migration is supported only for CMIP and PMIP.
4 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/AMS is in idle mode (e.g., when Idle mode MS/AMS moves or for other implementation reasons) requires that MS/AMS exit Idle mode and complete network reentry to complete MIP registration procedures [49]. If the MS/AMS 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 4-184 and Figure 4-186 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/AMS exits Idle mode after moving across ASNs. When the MS/AMS exits Idle mode due to incoming or outgoing data to/from the MS/AMS, 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/AMS 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/AMS 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.

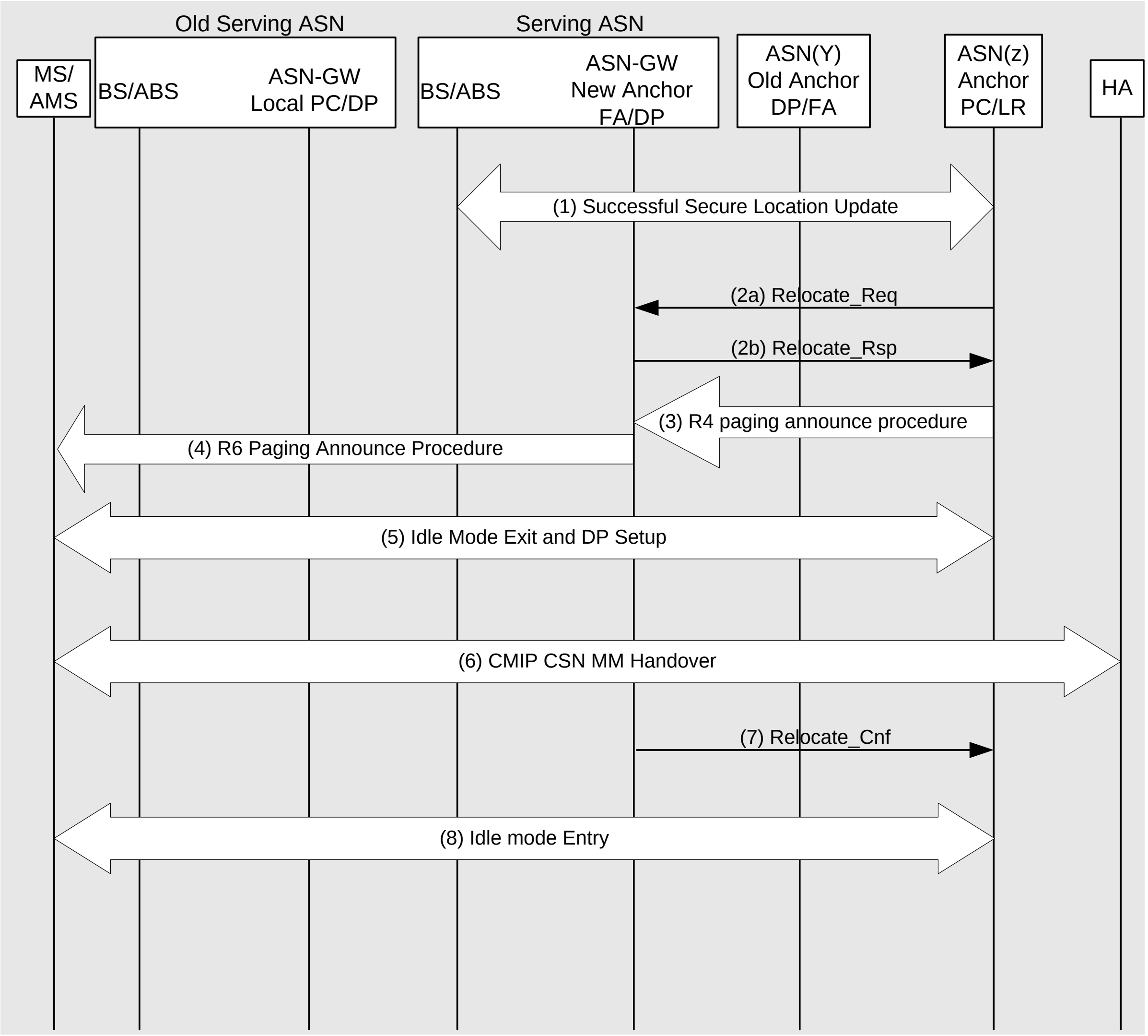


Figure 4-184 – FA Migration During Idle Mode: Anchor PC Initiated (Trigger to New FA)

STEP 1

The MS/AMS 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/AMS.

STEP 5

The MS/AMS performs idle mode exit procedures (as specified in section 4.10) 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/AMS 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/AMS 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.

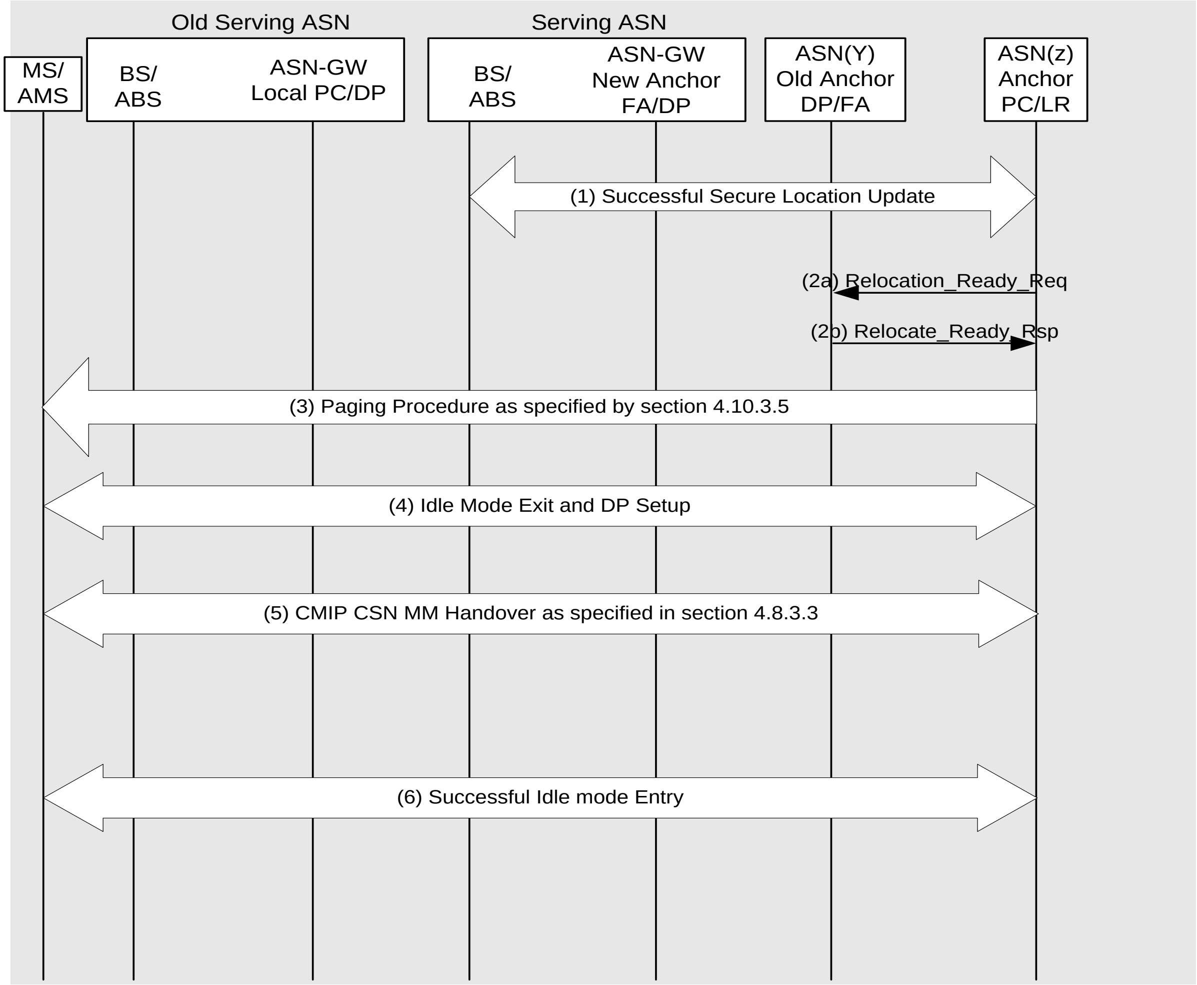

Old Serving ASN
Serving ASN
MS/ AMS
BS/ ABS
ASN-GW Local PC/DP
BS/ ABS
ASN-GW New Anchor FA/DP
ASN(Y) Old Anchor DP/FA
ASN(z) Anchor PC/LR
(1) Successful Secure Location Update
(2a) Relocation_Ready_Req
(2b) Relocate_Ready_Rsp
(3) Paging Procedure as specified by section 4.10.3.5
(4) Idle Mode Exit and DP Setup
(5) CMIP CSN MM Handover as specified in section 4.8.3.3
(6) Successful Idle mode Entry

Figure 4-185 – FA Migration During Idle Mode: Anchor PC Initiated (Trigger to Old FA)

STEP 1

The MS/AMS 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/AMS performs idle mode exit procedures (as specified in section 4.10) 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/AMS 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/AMS 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/AMS out of idle mode. Upon successful exit from idle mode, the new FA will send the Foreign Agent Advertisement message to the MS.

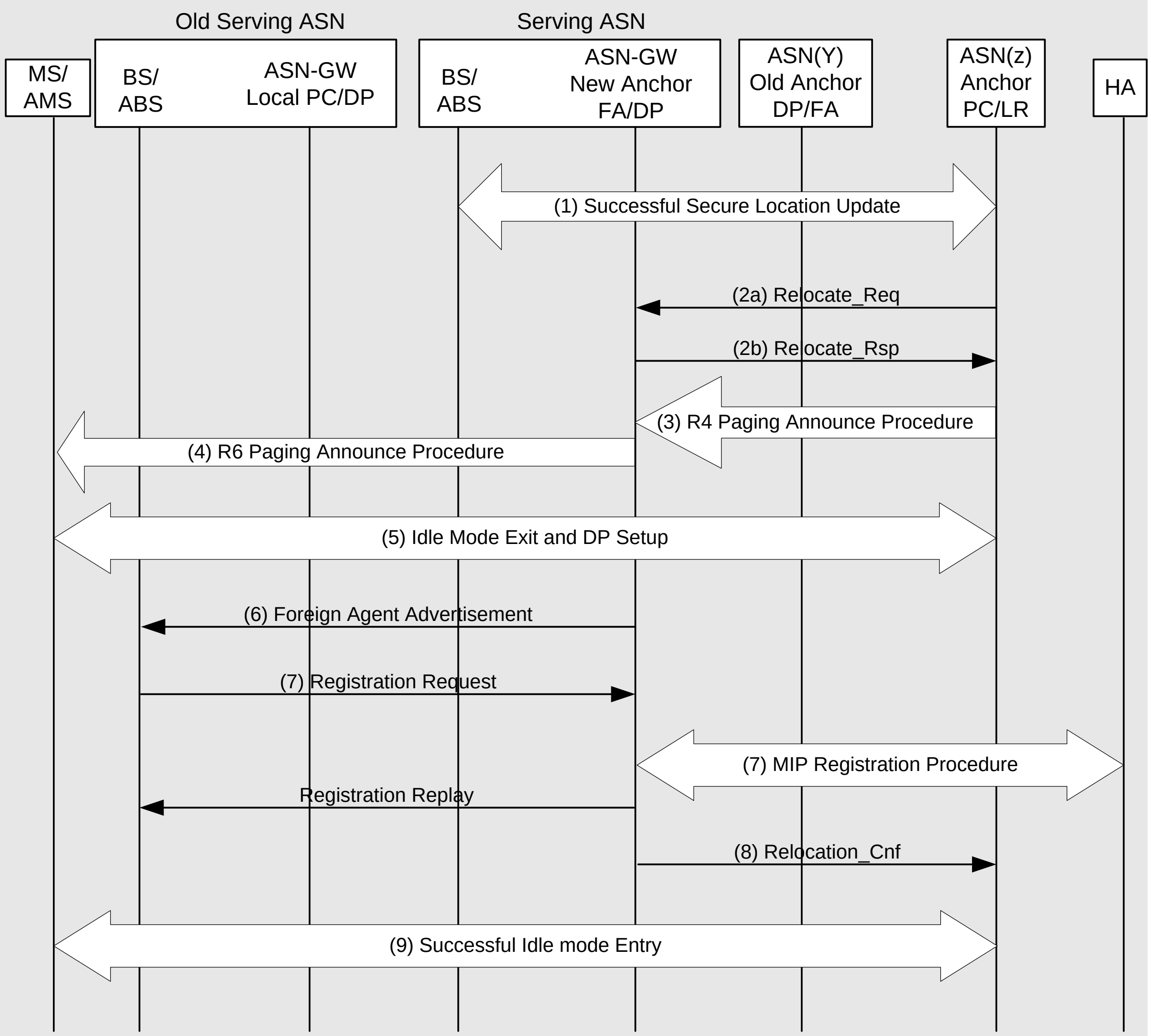


Figure 4-186 – FA Migration During Idle Mode: New (target) FA Initiated

STEP 1

The MS/AMS 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/AMS. 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/AMS 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/AMS.

STEP 5

The MS/AMS performs idle mode exit procedures (as specified in section 4.10) 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/AMS.

STEP 7

The MS/AMS 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/AMS.

STEP 8

Upon successful registration of the MS/AMS 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 4.10.5.2) to transition the MS/AMS to the idle mode.

4.10.6.3 PMIP4 in Idle Mode

Migration of FA for an Idle mode MS/AMS in a PMIP4 enabled ASN MAY be supported. The migration of the FA MAY be triggered when the MS/AMS 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 4.8.2.3.8.1. The two methods are identified to provide support for topologically aware and topologically unaware network models, but are not limited to such use.

Figure 4-187 illustrates the call flow for FA migration for an Idle Mode MS/AMS in a PMIP4 enabled ASN triggered by the Anchor PC-ASN.

Figure 4-188 illustrates the call flow for FA migration triggered by Target ASN (New FA) for an Idle Mode MS/AMS 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

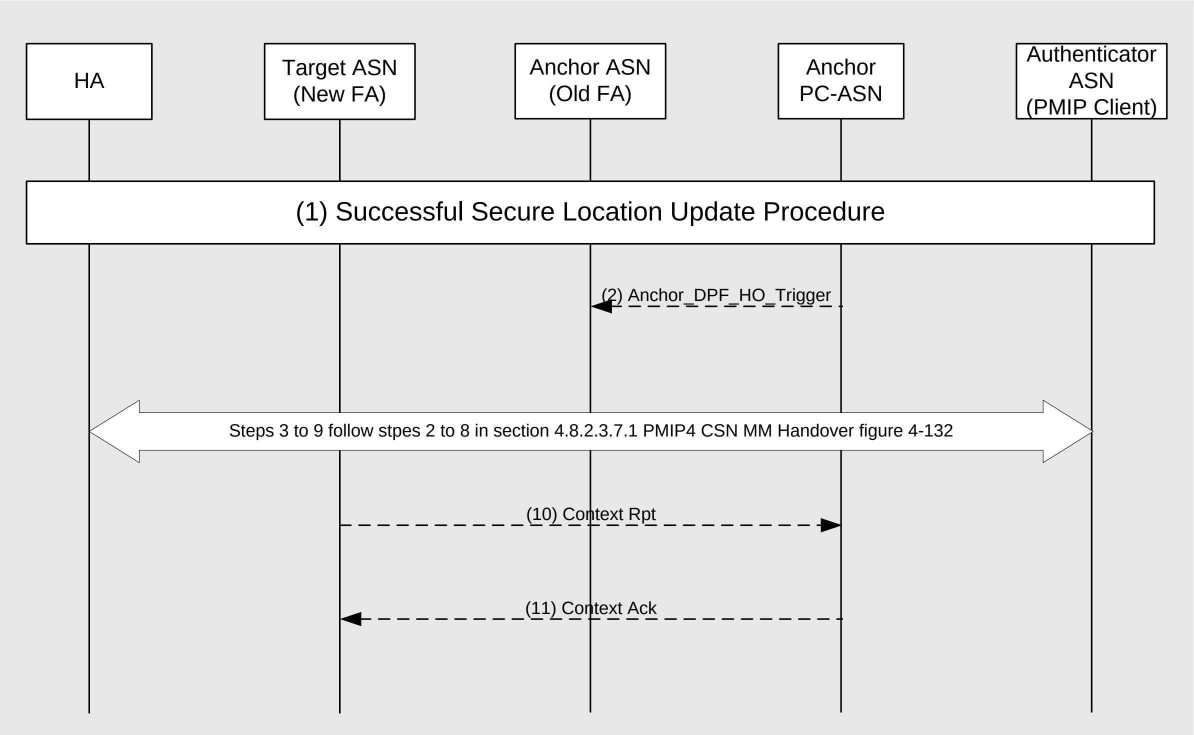

HA
Target ASN (New FA)
Anchor ASN (Old FA)
Anchor PC-ASN
Authenticator ASN (PMIP Client)
(1) Successful Secure Location Update Procedure
(2) Anchor_DPF_HO_Trigger
Steps 3 to 9 follow stpes 2 to 8 in section 4.8.2.3.7.1 PMIP4 CSN MM Handover figure 4-132
(10) Context Rpt
(11) Context Ack

Figure 4-187 – Anchor PC-ASN Triggered FA Migration for an Idle Mode MS/AMS 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 4.8.2.3.8.1 PMIP4 CSN MM Handover, Figure 4-144.

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/AMS 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)

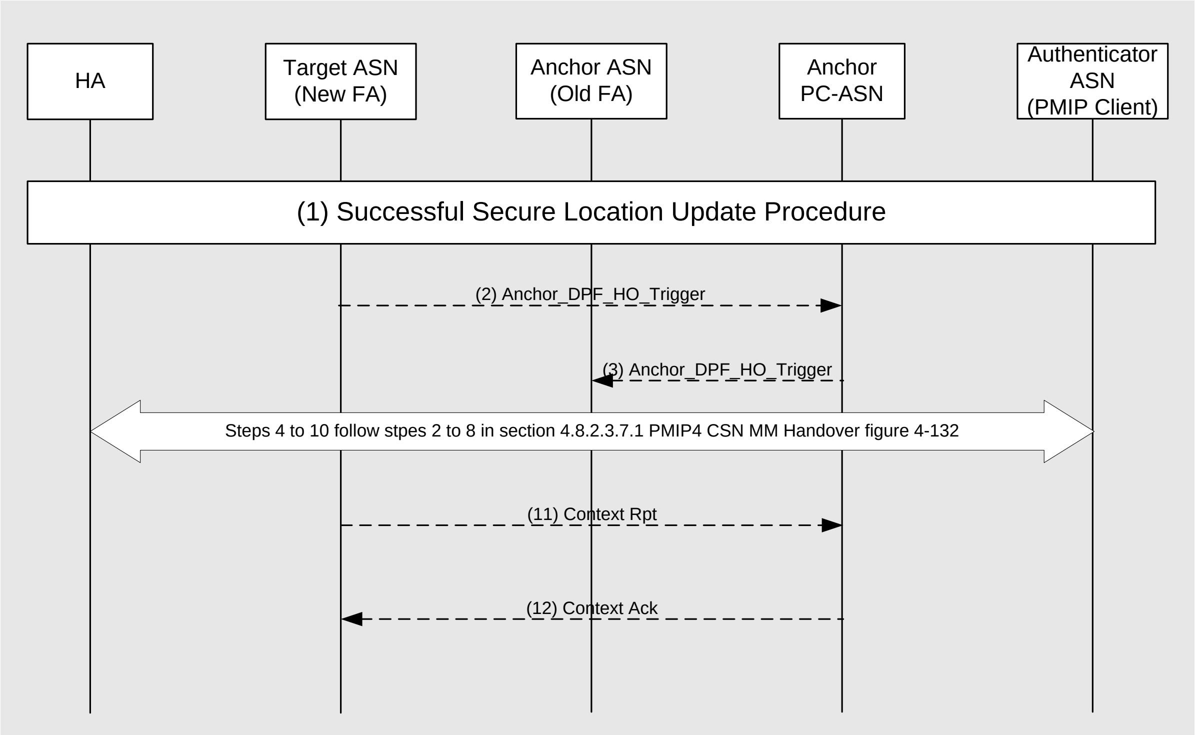

HA
Target ASN (New FA)
Anchor ASN (Old FA)
Anchor PC-ASN
Authenticator ASN (PMIP Client)
(1) Successful Secure Location Update Procedure
(2) Anchor_DPF_HO_Trigger
(3) Anchor_DPF_HO_Trigger
Steps 4 to 10 follow stpes 2 to 8 in section 4.8.2.3.7.1 PMIP4 CSN MM Handover figure 4-132
(11) Context Rpt
(12) Context Ack

Figure 4-188 – Target ASN (New FA) Triggered FA Migration for an Idle Mode MS/AMS 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 4.8.2.3.8.1 PMIP4 CSN MM Handover, Figure 4-144.

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/AMS related context with New FA for the MS/AMS.

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/AMS 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/AMS'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.

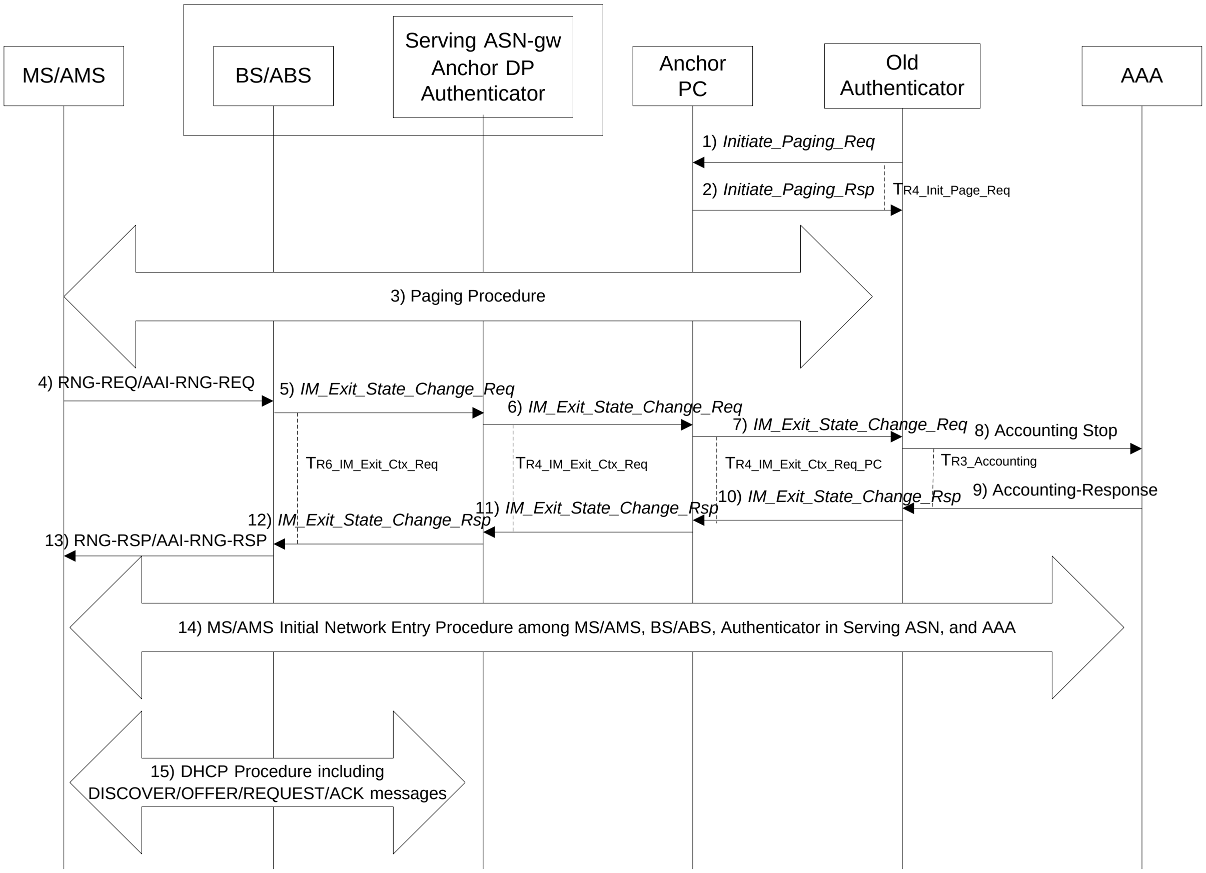

MS/AMS
BS/ABS
Serving ASN-gw Anchor DP Authenticator
Anchor PC
Old Authenticator
AAA
1) Initiate_Paging_Req
2) Initiate_Paging_Rsp
TR4_Init_Page_Req
3) Paging Procedure
4) RNG-REQ/AAI-RNG-REQ
5) IM_Exit_State_Change_Req
6) IM_Exit_State_Change_Req
7) IM_Exit_State_Change_Req
8) Accounting Stop
TR6_IM_Exit_Ctx_Req
TR4_IM_Exit_Ctx_Req
TR4_IM_Exit_Ctx_Req_PC
TR3_Accounting
9) Accounting-Response
10) IM_Exit_State_Change_Rsp
11) IM_Exit_State_Change_Rsp
12) IM_Exit_State_Change_Rsp
13) RNG-RSP/AAI-RNG-RSP
14) MS/AMS Initial Network Entry Procedure among MS/AMS, BS/ABS, Authenticator in Serving ASN, and AAA
15) DHCP Procedure including DISCOVER/OFFER/REQUEST/ACK messages

Figure 4-189 – 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/AMS. 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. 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.

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.

STEP 13

When the BS/ABS receives this message, it sends RNG-RSP with HO Process Optimization TLV or AAI-RNG-RSP with Reentry Process Optimization in order for MS/AMS to perform Full network entry and DHCP procedure according to [13].

Note that BS/ABS SHALL set the HO optimization TLV/Reentry Process Optimization settings to "Full network entry with traffic IP address refresh".

STEP 14

MS/AMS, BS/ABS, Authenticator and AAA performs Step 3 to Step 28 of MS/AMS initiated Network Entry procedure as described in the section 4.5.1.1. 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/AMS 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/AMS in a PMIP6 enabled ASN MAY be supported. The migration of the AR/MAG MAY be triggered when the MS/AMS moves across ASNs.

Figure 4-190 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.

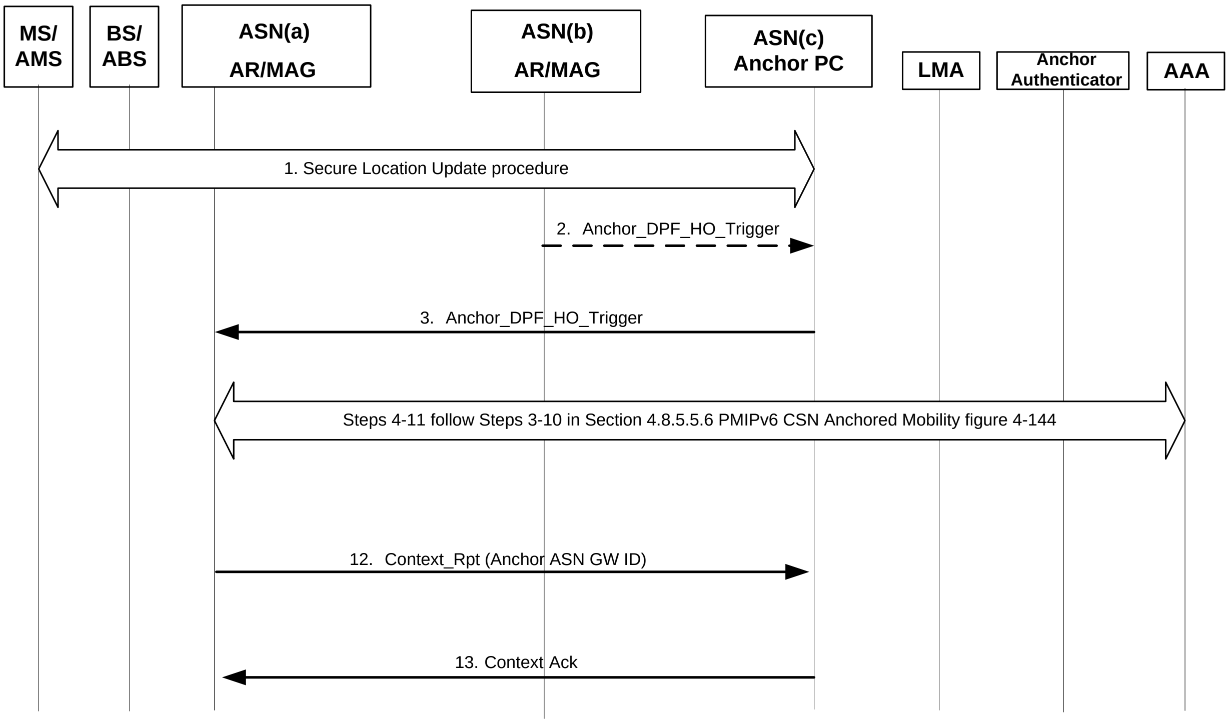

MS/ AMS
BS/ ABS
ASN(a) AR/MAG
ASN(b) AR/MAG
ASN(c) Anchor PC
LMA
Anchor Authenticator
AAA
1. Secure Location Update procedure
2. Anchor_DPF_HO_Trigger
3. Anchor_DPF_HO_Trigger
Steps 4-11 follow Steps 3-10 in Section 4.8.5.5.6 PMIPv6 CSN Anchored Mobility figure 4-144
12. Context_Rpt (Anchor ASN GW ID)
13. Context Ack

Figure 4-190 – PMIP6 AR/MAG Migration for an Idle Mode MS/AMS

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 4-193).

STEP 13

The Anchor PC-ASN sends *Context_Ack* to Anchor ASN (old AR/MAG) and updates the MS/AMS related context with the new AR/MAG for the MS/AMS.

Table 4-193 – 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 [91] 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 [88]. 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.

An MS/AMS is considered “dual-stack capable” if it has the capability to support simultaneous IPv4 and IPv6 end-to-end connectivity via WiMAX networks. An MS/AMS is considered “dual-stack enabled” when it is configured with at least one IPv4 address and at least one IPv6 address. Consequently, a dual-stack capable MS/AMS may not be dual-stack enabled if, for example, it has only an IPv4 address configured. In this specification, the term “dual-stack MS/AMS” will be used as a short form of “dual-stack capable MS/AMS.”

4.11.1 Network Model

The default IPv6 router or 1st hop router from the MS/AMS 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/AMS autoconfigures an address based on the prefix advertised by the AR or is assigned an address via DHCPv6 or FIAA. This address is based on the prefix that topologically may belong to the Home CSN of the MS/AMS, 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/AMS. Figure 4-191 shows the network model for IPv6.

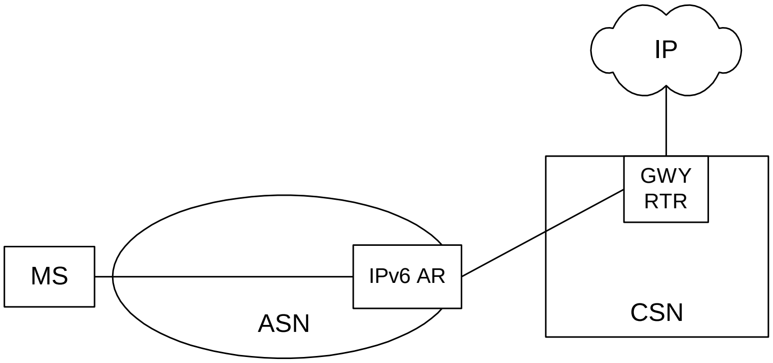


Figure 4-191 – IPv6 Network Model

4.11.2 Point to Point Link Between the MS/AMS and AR

The link between the MS/AMS 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/ABS and AR forms the point-to-point link. With the point-to-point type of link underlying the IPv6 layer, each MS/AMS is assigned one or more unique IPv6 prefixes. The only entities on the link are the MS/AMS and the AR. The granularity of the GRE tunnel between the BS/ABS 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/AMS 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/AMS 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/AMS 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/AMS and the access router in the ASN. On completion of the establishment of the ISF, router advertisements and address assignment procedures are initiated (unless already handled via FIAA). The successful establishment of the IPv6 ISF can be viewed as the trigger for the AR to send the router advertisement. The MS/AMS 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 PMIP6 service separate RADIUS attributes SHALL be used to boostrap 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/AMS. 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/AMS NAI to select an appropriate pool.

An MS/AMS receives an RA from the AR on completion of the establishment of the IPv6 ISF. An MS/AMS may also send router solicitations on completion of the establishment of the ISF. If the MS/AMS does not receive an unsolicited RA from the AR or in response to a router solicitation, the MS/AMS will initiate network exit and re-entry procedures.

An MS/AMS 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/AMS, as a unique link and manages it as a separate (virtual) interface per link.

The IPv6 prefix assigned to an MS/AMS may be used as the classifier at the AR for the downlink associated with the MS/AMS. 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 IEEE 802.16m-specific mechanism (FIAA) and IETF-specified mechanisms [32].

- Fast IP Address Allocation –FIAA [105])
- IPv6 Addressing Architecture – [50] (Updated by [59])
- IPv6 stateless address autoconfiguration – [79]
- Privacy Extensions for Address Configuration in IPv6 – [44]
- Default Address Selection for IPv6 – RFC 3484
- Stateful Address Autoconfiguration – DHCPv6, [48]

The node requirements [32] 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/AMS 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/AMS for address autoconfiguration. The IID is generated by the MS/AMS 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:

IPv6 Prefix (64 bits)	Interface Identifier (64 bits)

Figure 4-192 – 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.

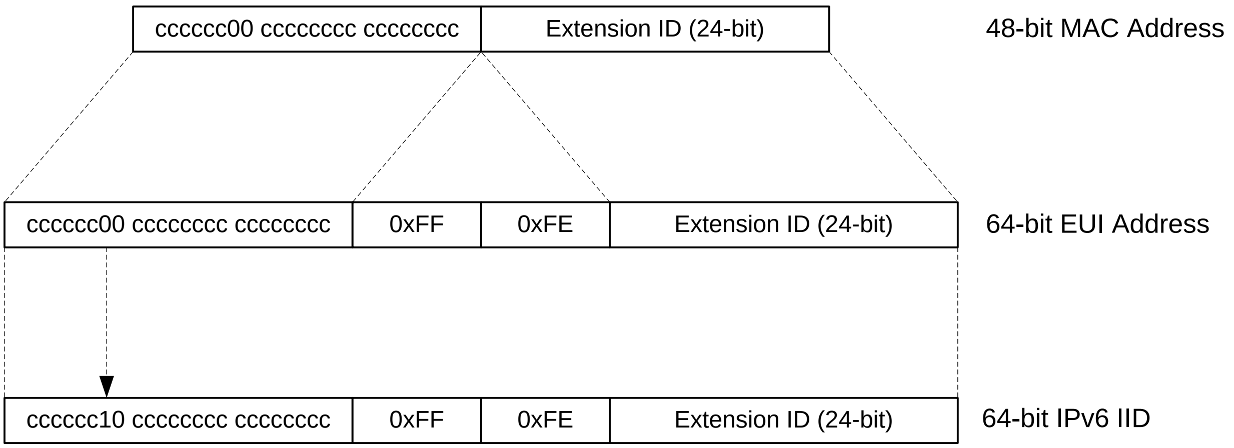


Figure 4-193 – Illustration of Forming the IID

For addresses that are based on privacy extensions, the MS/AMS may generate random IIDs as specified in RFC3041.

4.11.4.2 Duplicate Address Detection (DAD)

DAD is performed as per RFC 2461, [28].

4.11.4.3 Stateless Address Auto-configuration

Stateless address auto-configuration is performed as per RFC 2461, [28]. The access router in the ASN is the default router that advertises a prefix that is used by the MS/AMS to configure an address.

4.11.4.4 Stateful Address Auto-configuration

4.11.4.4.1 DHCP

If the M-flag is set in the RA message from the access router to the MS/AMS, the MS/AMS MAY perform stateful address autoconfiguration if it hasn't already used FIAA. For this purpose, the MS/AMS SHALL use DHCPv6 procedures as defined in [48]. The MS/AMS 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/AMS 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 [48].

4.11.4.4.2 FIAA

If the AMS decides to use FIAA, it can do so during the IEEE 802.16m registration procedure. AMS obtains the IP address and possibly other configuration parameters (e.g., DNS) during AAI-REG-REQ/RSP procedure and configures them on its IP stack as soon as ISF(s) is/are established.

4.11.5 DNS Discovery

In order to be able to use the Domain Name Service (DNS), the MS/AMS has to be configured with the IPv6 DNS server addresses. The standard mechanisms for dynamically configuring the DNS server addresses is via Dynamic Host Configuration Protocol (DHCP) for IPv6 using DNS Configuration options [Reference to RFC 3646] and FIAA.

Choosing the right DNS Server configuration method is dependent on the address allocation mechanisms. If stateful address auto-configuration is used; then either DHCPv6 or FIAA 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/AMS MAY use DHCPv6 DNS Configuration Options [RFC3646] – either with DHCPv6 [48] when stateful address configuration is used, or Stateless DHCPv6[RFC3736] when stateless address auto-configuration is used.

The network SHALL support DHCPv6 [48] and DHCPv6 DNS Configuration Options [RFC3646] when stateful address auto-configuration, is used. The network SHALL support stateless DHCPv6 [48] with the DNS Configuration options [RFC3646] when stateless address auto-configuration is used.

4.11.5.2 DNS configuration via FIAA

FIAA is also based on using DHCP options. These options are carried over the AAI-REG-REQ/RSP procedure when used with FIAA. Additional-Host-configurations IE is used for encapsulating these DHCP options over AAI-REQ-RSP message. DHCP options mentioned in 4.11.5.1 are also applicable for FIAA usage.

4.11.6 Uplink and Downlink Transmission of IPv6 Packets

4.11.6.1 Uplink

IPv6 packets can be sent by the MS/AMS 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/AMS 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/ABS receives the IPv6 packet. Based on the CID that the packet was received on, the BS/ABS has a mapping to a service flow which maps to a Data Path ID (GRE key). The BS/ABS 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/AMS 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/ABS. When the BS/ABS receives the IPv6 packet the BS/ABS forwards the IPv6 packet on a transport connection identified by a CID to the appropriate MS/AMS using the mapping of the SFID to the transport connection. The BS/ABS 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/AMS to be assigned a new prefix and hence a new address. However, in case of PMIP6 the MS/AMS 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/AMS is determined by a functional entity in the ASN. AR relocation also causes the MS/AMS to update its binding with an HA in the case of Mobile IPv6. The decision to relocate the AR for an MS/AMS is always controlled by the network. The types of triggers that can cause AR/R3 relocation are:

c. MS/AMS mobility: The MS/AMS hands off to a new Base Station under a new Access Router.

d. Wake-up from idle mode: The MS/AMS wakes up from the idle mode under a different Access Router than the one under which it entered the idle mode.

e. Resource optimization: The network decides for resource optimization purposes to transfer the R3 endpoint for the MS/AMS from the serving Access Router to a new Access Router.

AR relocation for an MS/AMS requires the MS/AMS to perform network re-entry procedure in the scenario the MS/AMS 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/AMS 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/AMS 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 flows describes the R4/R6 Data Path Pre-Registration procedure.

4.12.1.1.1 R4/R6 Data Path Pre-Registration Procedure Initiated by Target BS

A Data Path Pre-Registration is initiated by the Target BS(s).

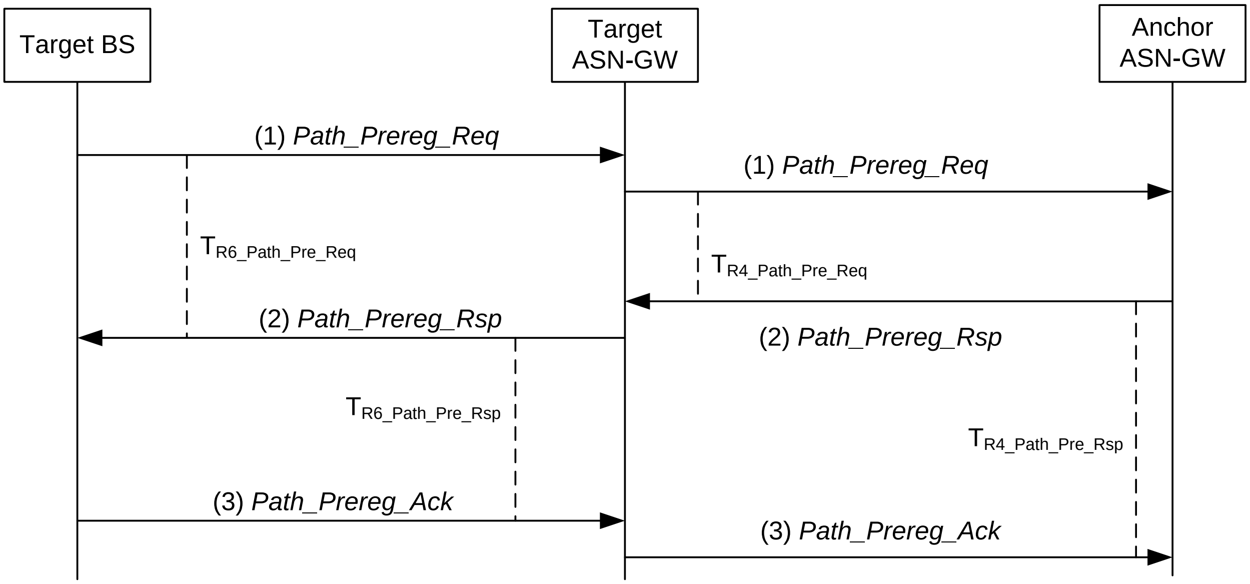


Figure 4-194 – R4/R6 Data Path Pre-Registration Procedure initiated by Target BS

STEP 1

The Target BS initiates the 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 $T_{R4\_Path\_Pre\_Req}$.

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, the Target BS stops timer $T_{R6\_Path\_Pre\_Req}$.

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 $T_{R4\_Path\_Pre\_Rsp}$.

4.12.1.1.2 R4/R6 Data Path Pre-Registration Procedure Initiated by Anchor ASN-GW (only applies to BS buffer switching DI HO)

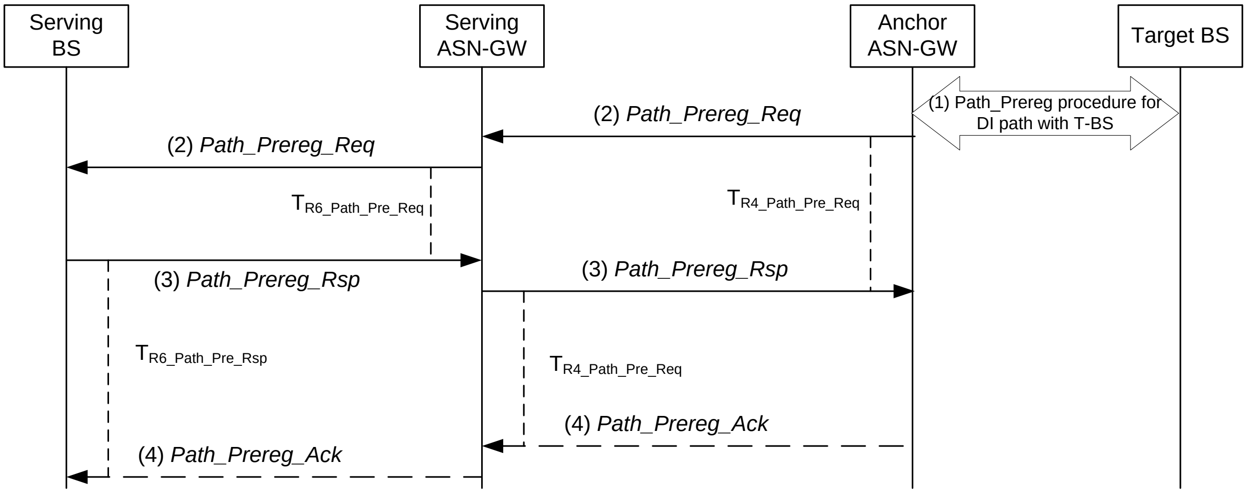


Figure 4-195 – R4/R6 Data Path Pre-Registration Procedure initiated by Anchor ASN-GW for BS buffer switching DI

Note: this section is for BS buffer switching data integrity method with data delivery via ASN-GW. For more details, see section 4.7.8.3.1.3.1.

STEP 1

The Target BS starts the Path_Preregistration procedure with Anchor GW for a Data Integrity data path establishment.

STEP 2

Upon receipt of the data path pre-registration request from the Target BS, the anchor ASN-GW initiates pre-establishment of the data path for an MS by sending a R4 *Path_Prereg_Req* message, which includes the data path information to the ASN-GW and starts timer $T_{R4\_Path\_Pre\_Req}$.

The ASN-GW initiates pre-establishment of the data path for an MS by sending an *Path_Prereg_Req* message which includes the data path information to the serving BS and starts timer $T_{R6\_Path\_Pre\_Req}$.

STEP 3

The serving BS sends a *Path_Prereg_Rsp* message to the ASN-GW and starts timer $T_{R6\_Path\_Pre\_Rsp}$. Upon receipt of the *Path_Prereg_Rsp* message, the ASN-GW stops timer $T_{R6\_Path\_Pre\_Req}$.

The ASN-GW sends a *Path_Prereg_Rsp* message to the Anchor ASN-GW and starts timer $T_{R4\_Path\_Pre\_Rsp}$.

STEP 4

The Anchor ASN-GW sends a *Path_Prereg_Ack* message to the ASN-GW. Upon receipt of the *Path_Prereg_Ack* message, the ASN-GW stops timer $T_{R4\_Path\_Pre\_Rsp}$.

The ASN-GW sends a *Path_Prereg_Ack* message to the serving BS. Upon receipt of the *Path_Prereg_Ack* message, the serving BS stops timer $T_{R6\_Path\_Pre\_Rsp}$.

4.12.1.2 R6 Data Path Pre-Registration Procedure

The following call flow describes the R6 Path Pre-Registration procedure during handovers.

4.12.1.2.1 Data Path Pre-Registration Procedure Initiated by Target BS

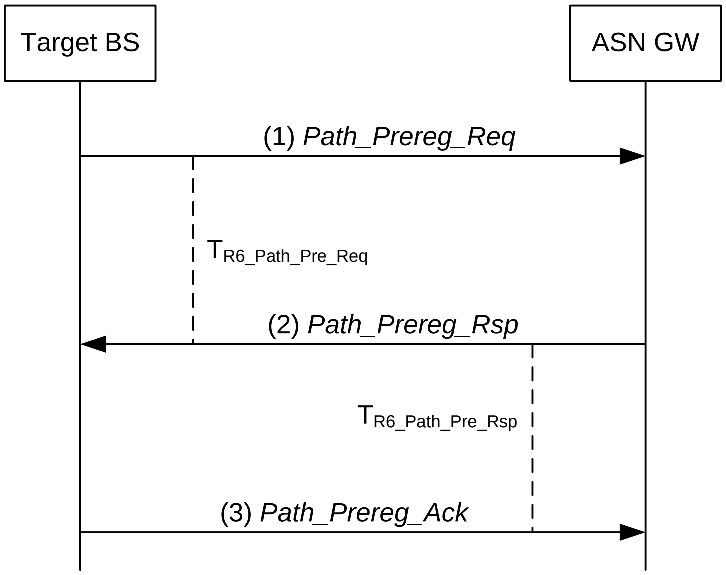


Figure 4-196 – R6 Data Path Pre-Registration Procedure initiated by Target BS

STEP 1

The Target BS initiates a pre-establishment of the data path for an MS by sending a *Path_Prereg_Req* message to the ASN-GW and starts timer $T_{R6\_Path\_Pre\_Req}$.

STEP 2

The 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, the Target BS stops timer $T_{R6\_Path\_Pre\_Req}$.

STEP 3

The Target BS sends a *Path_Prereg_Ack* message to the ASN-GW. Upon receipt of the *Path_Prereg_Ack* message, the ASN-GW stops timer $T_{R6\_Path\_Pre\_Rsp}$.

4.12.1.2.2 Data Path Pre-Registration Procedure Initiated by ASN GW (only applies for BS buffer switching DI HO)

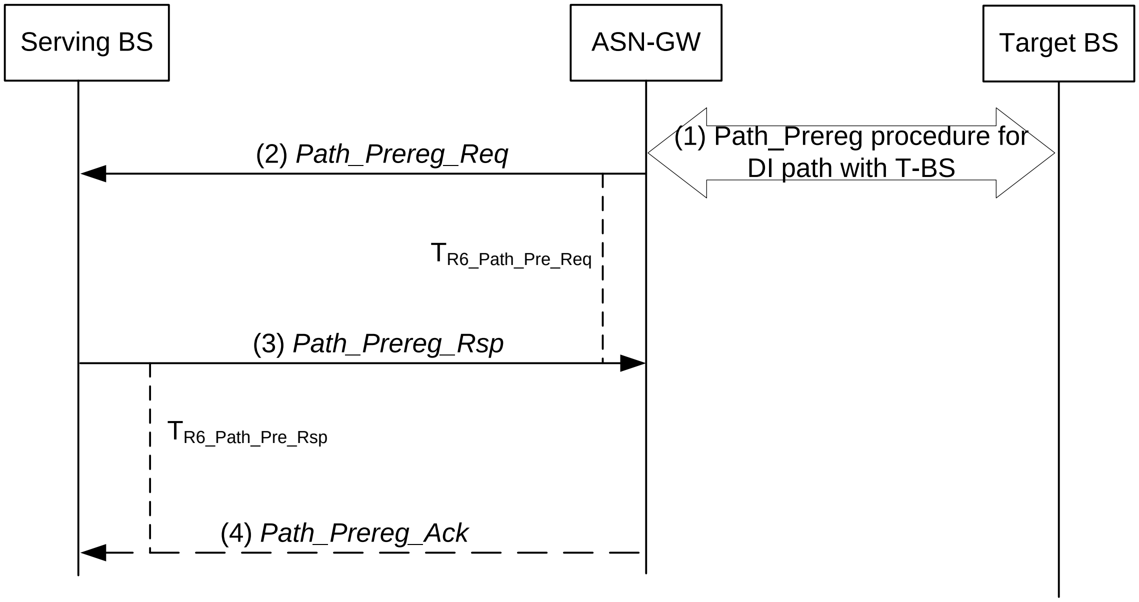


Figure 4-197 – R6 Data Path Pre-Registration Procedure initiated by ASN-GW for BS buffer switching DI HO

STEP 1

The Target BS starts the Path_Preregistration procedure with the ASN GW for Data Integrity data path establishment.

STEP 2

Upon receipt of the data path pre-registration request from the Target BS, the ASN-GW initiates pre-establishment of the data path for an MS by sending a *Path_Prereg_Req* message to the serving BS and starts timer $T_{R6\_Path\_Pre\_Req}$.

STEP 3

The serving BS sends a *Path_Prereg_Rsp* message to the ASN-GW and starts timer $T_{R6\_Path\_Pre\_Rsp}$. Upon receipt of the *Path_Prereg_Rsp* message, the ASN-GW stops timer $T_{R6\_Path\_Pre\_Req}$.

STEP 4

The ASN-GW sends a *Path_Prereg_Ack* message to the serving BS. Upon receipt of the *Path_Prereg_Ack* message, the serving BS 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 R4/R6 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.

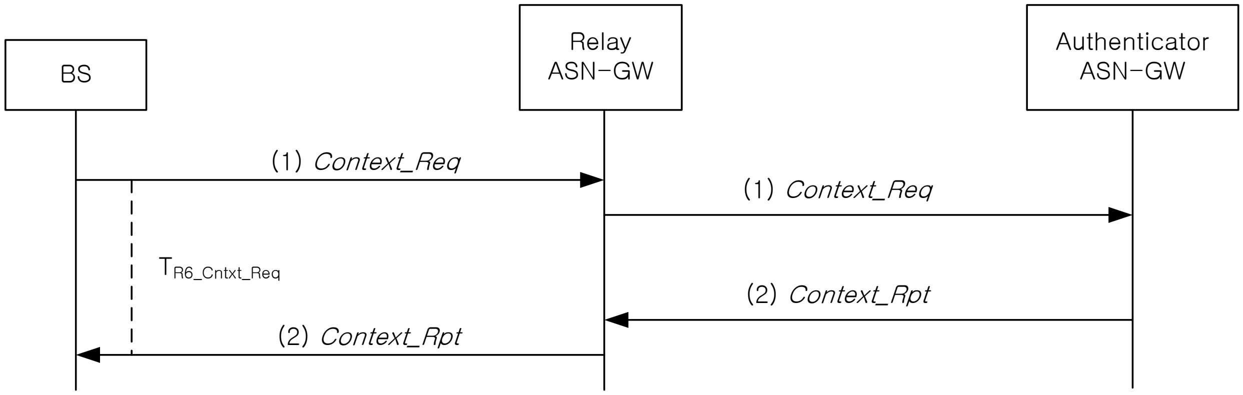


Figure 4-198 – R4/R6 Context Retrieval Procedure

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 $T_{R4\_Cntxt\_Req.}$

The Authenticator ASN-GW responds by sending the requested context information for the MS 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 MS in the *Context_Rpt* message. The Relay ASN-GW relays the message to the BS 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 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.

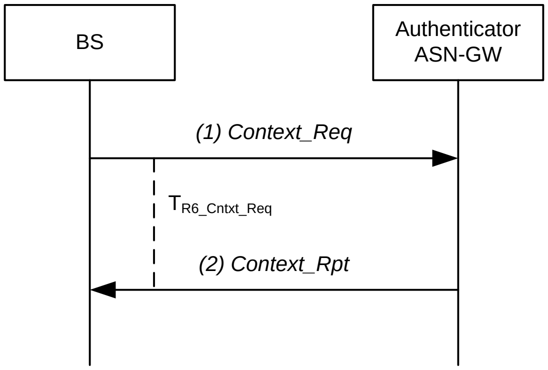


Figure 4-199 – R6 Context Retrieval Procedure

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 $T_{R6\_Cntxt\_Req.}$

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 flows 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.

4.12.3.1.1 R4/R6 Data Path Registration Procedure Initiated by Target BS

The Data Path Pre-Registration procedure may be initiated by the Target BS(s).

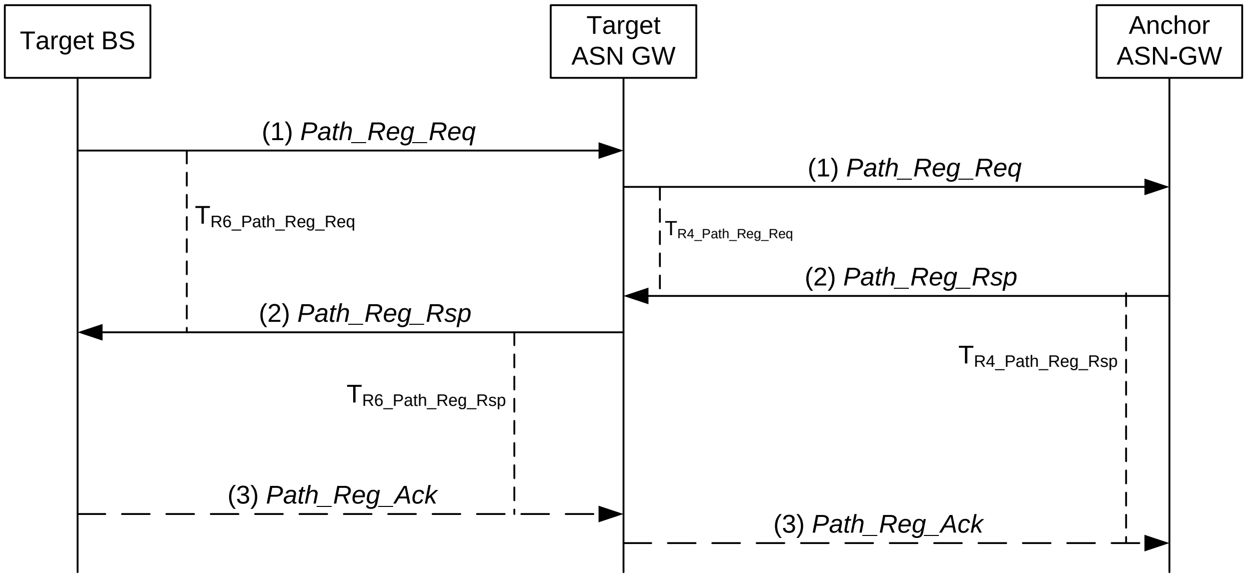


Figure 4-200 – R4/R6 Data Path Registration Procedure initiated by Target BS

STEP 1

The Target BS initiates a Data Path Registration procedure by sending a *Path_Reg_Req* message to the Target ASN-GW and starts timer $T_{R6\_Path\_Reg\_Req}$.

The Target ASN-GW initiates a Data Path Registration procedure by sending a *Path_Reg_Req* message to the Anchor ASN and starts timer $T_{R4\_Path\_Reg\_Req}$.

STEP 2

The Anchor ASN-GW sends a *Path_Reg_Rsp* message to the Target ASN-GW. The Anchor ASN-GW starts timer $T_{R4\_Path\_Reg\_Rsp}$, 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, the Target ASN-GW stops timer $T_{R4\_Path\_Reg\_Req}$.

The Target ASN GW sends a *Path_Reg_Rsp* message to the Target BS and, if no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, starts timer $T_{R6\_Path\_Reg\_Rsp.}$ Upon receipt of the *Path_Reg_Rsp* message, the Target BS stops timer $T_{R6\_Path\_Reg\_Req}$.

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 the Target ASN-GW. Upon receipt of the *Path_Reg_Ack* message, the Target ASN-GW stops timer $T_{R6\_Path\_Reg\_Rsp}$.

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction then the Target ASN-GW sends a *Path_Reg_Ack* message to the Anchor ASN-GW. Upon receipt of the *Path_Reg_Ack* message, the Anchor ASN-GW stops timer $T_{R4\_Path\_Reg\_Rsp}$.

4.12.3.1.2 R4/R6 Data Path Registration Procedure Initiated by Anchor ASN-GW (only applies to BS buffer switching DI HO

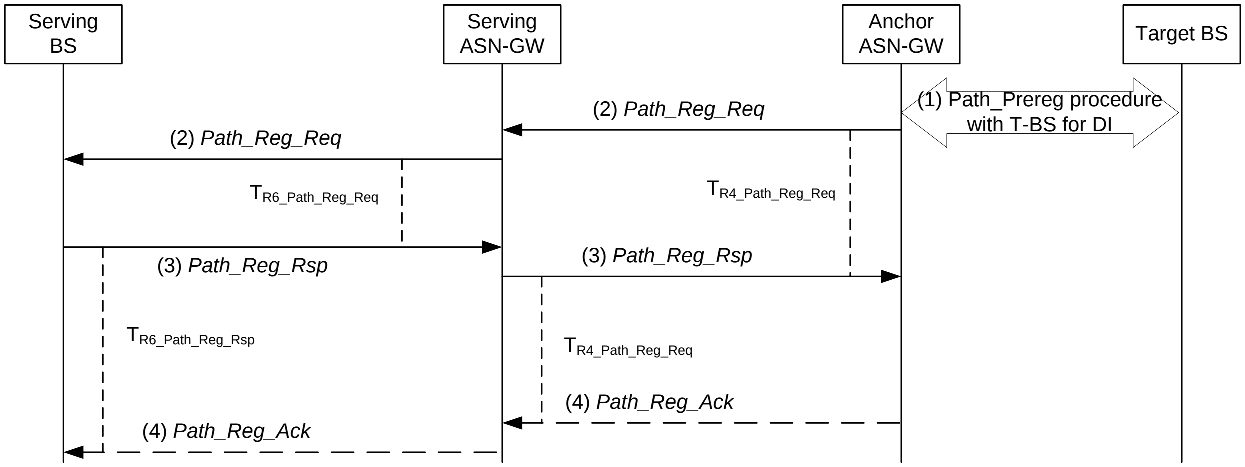


Figure 4-201 – R4/R6 Data Path Registration Procedure initiated by Anchor ASN-GW for BS buffer switching DI

Note: this section is for BS buffer switching data integrity method with data delivery via ASN-GW. For more details, see section 4.7.8.3.1.3.1.

STEP 1

The Target BS starts the Path_Registration procedure with Anchor GW for a Data Integrity data path establishment.

STEP 2

Upon receipt of the data path registration request from the Target BS, the anchor ASN-GW initiates a Data Path Registration procedure by sending a *Path_Reg_Req* message to the Serving ASN-GW and starts timer $T_{R4\_Path\_Reg\_Req}$.

The Serving ASN-GW initiates a Data Path Registration procedure by sending a *Path_Reg_Req* message to the serving BS and starts timer $T_{R6\_Path\_Reg\_Req}$.

STEP 3

The Serving BS sends a *Path_Reg_Rsp* message to the Serving ASN-GW. The Serving BS starts timer $T_{R6\_Path\_Reg\_Rsp}$, 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, the Target ASN-GW stops timer $T_{R4\_Path\_Reg\_Req}$.

The Serving ASN-GW sends a *Path_Reg_Rsp* message to the Anchor ASN-GW and, if no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, it starts timer $T_{R4\_Path\_Reg\_Rsp}$. Upon receipt of the *Path_Reg_Rsp* message, the Anchor ASN-GW stops timer $T_{R6\_Path\_Reg\_Req}$.

STEP 4

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction the Anchor ASN-GW sends a *Path_Reg_Ack* message to the Target ASN-GW. Upon receipt of the *Path_Reg_Ack* message, the ASN-GW stops timer $T_{R4\_Path\_Reg\_Rsp}$.

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, the Serving ASN-GW sends a *Path_Reg_Ack* message to BS. Upon receipt of the *Path_Reg_Ack* message, the Serving BS stops timer $T_{R6\_Path\_Reg\_Rsp}$.

4.12.3.2 R6 Data Path Registration Procedure

Data Path Registration procedure takes place between the Target BS and the ASN-GW immediately after the MS has arrived at the Target BS.

4.12.3.2.1 Data Path Registration Procedure Initiated by Target BS

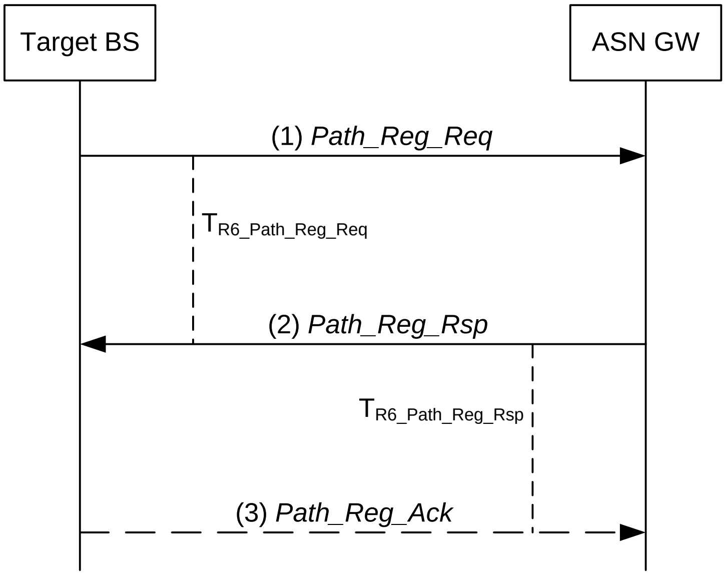


Figure 4-202 – Data Path Registration Procedure initiated by Target BS

STEP 1

The Target BS initiates a Data Path Registration procedure by sending a *Path_Reg_Req* message to the ASN-GW and starts timer $T_{R6\_Path\_Reg\_Req}$.

STEP 2

The ASN-GW sends a *Path_Reg_Rsp* message to the Target BS and, if no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, it starts timer $T_{R6\_Path\_Reg\_Rsp.}$ Upon receipt of the *Path_Reg_Rsp* message, the Target BS stops timer $T_{R6\_Path\_Reg\_Req.}$

STEP 3

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, the Target BS sends a *Path_Reg_Ack* message to the ASN-GW. Upon receipt of the *Path_Reg_Ack* message, the ASN-GW stops timer $T_{R6\_Path\_Reg\_Rsp}$.

4.12.3.2.2 Data Path Registration Procedure Initiated by ASN GW (only applies to BS buffer switching DI HO)

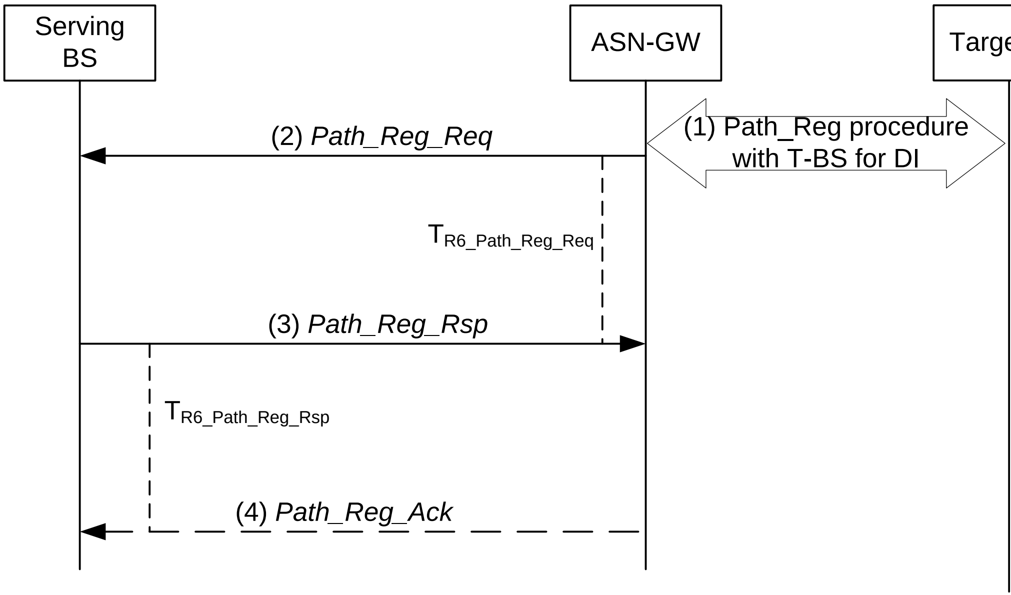


Figure 4-203 – R6 Data Path Registration Procedure initiated by ASN-GW for BS buffer switching DI HO

STEP 1

The Target BS starts the Path_Registration procedure with the ASN-GW for Data Integrity data path establishment.

STEP 2

Upon receipt of the data path registration request from the Target BS, the ASN-GW initiates a Data Path Registration procedure by sending a *Path_Reg_Req* message to the Serving BS and starts timer $T_{R6\_Path\_Reg\_Req}$.

STEP 3

The Serving BS sends a *Path_Reg_Rsp* message to the ASN-GW and, if no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, it starts timer $T_{R6\_Path\_Reg\_Rsp}$. Upon receipt of the *Path_Reg_Rsp* message, the ASN-GW stops timer $T_{R6\_Path\_Reg\_Req}$.

STEP 4

If no Data Path Pre-Registration procedure has been completed prior to the Data Path Registration transaction, the ASN-GW sends a *Path_Reg_Ack* message to the Serving BS. Upon receipt of the *Path_Reg_Ack* message, the Serving BS stops timer $T_{R6\_Path\_Reg\_Rsp}$.

4.12.4 R4 Data Path De-Registration Procedure

4.12.4.1 R4/R6 Data Path De-Registration Procedure

The following call flows describe the R4/R6 Data Path De-Registration procedure.

4.12.4.1.1 R4/R6 Data Path De-Registration Procedure Initiated by Anchor ASN-GW

R4/R6 Data Path De-Registration may be initiated by the Anchor ASN-GW.

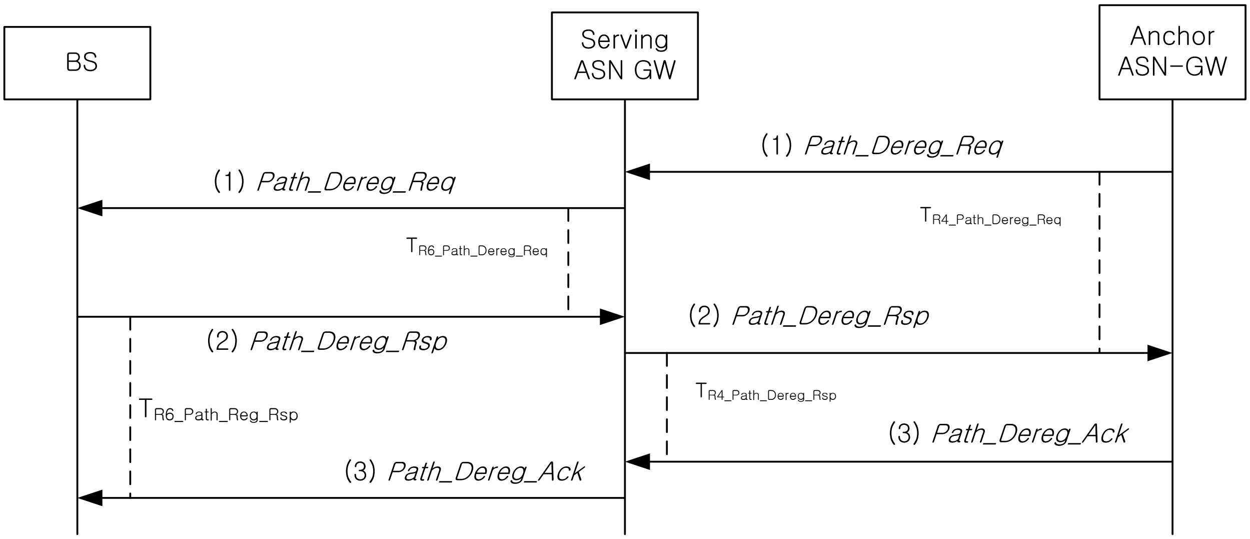


Figure 4-204 – R4/R6 Data Path De-Registration Procedure initiated by Anchor ASN-GW

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 $T_{R4\_Path\_Dereg\_Req}$.

Serving ASN-GW initiates Data Path De-Registration procedure by sending a *Path_Dereg_Req* message to BS and starts timer $T_{R6\_Path\_Dereg\_Req}$.

STEP 2

BS sends a *Path_Dereg_Rsp* message to Serving ASN-GW and starts $T_{R6\_Path\_De\text{-}Reg\_Rsp}$. Upon receipt of the *Path_Dereg_Rsp* message, Serving ASN-GW stops timer $T_{R6\_Path\_Dereg\_Req}$.

Serving ASN-GW sends a *Path_Dereg_Rsp* message to Anchor ASN-GW and starts timer $T_{R4\_Path\_Dereg\_Rsp}$. Upon receipt of the *Path_Dereg_Rsp* message, Anchor ASN-GW stops timer $T_{R4\_Path\_Dereg\_Req}$.

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 $T_{R4\_Path\_Dereg\_Rsp}$.

Serving ASN-GW sends a *Path_Dereg_Rsp* message to BS. Upon receipt of the *Path_Dereg_Rsp* message, BS stops timer $T_{R6\_Path\_Dereg\_Rsp}$.

4.12.4.1.2 R4/R6 Data Path De-Registration Procedure Initiated by BS

R4/R6 Data Path De-Registration may be initiated by the BS.

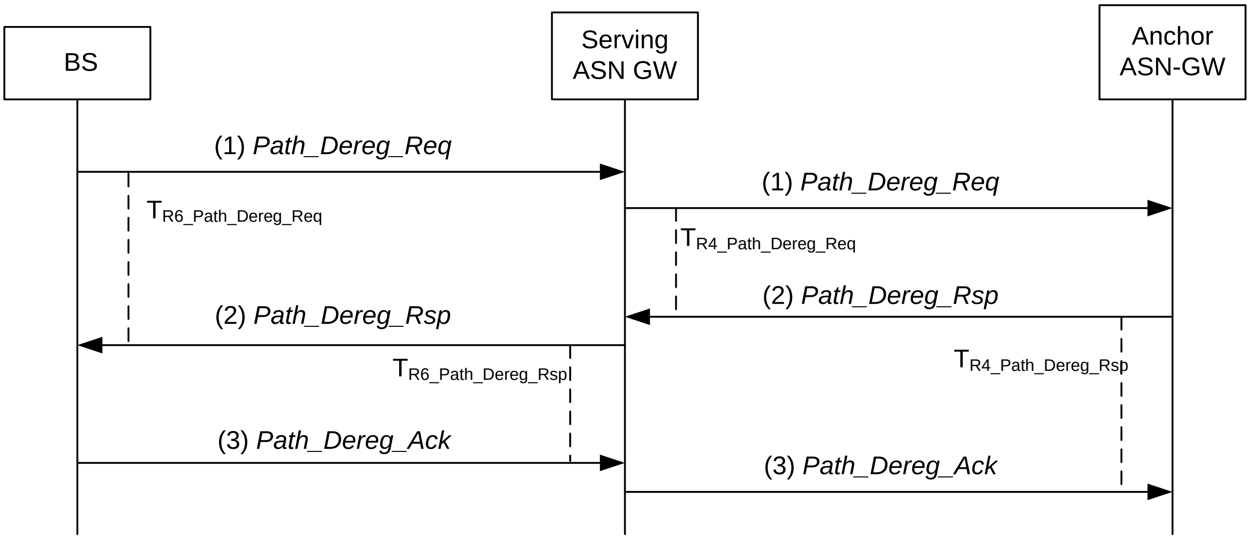


Figure 4-205 – R4/R6 Data Path De-Registration Procedure initiated by BS

STEP 1

BS initiates Data Path De-Registration procedure by sending a *Path_Dereg_Req* message to Serving ASN-GW and starts timer $T_{R6\_Path\_Dereg\_Req}$.

Serving ASN-GW initiates Data Path De-Registration procedure by sending a *Path_Dereg_Req* message to Anchor ASN-GW and starts timer $T_{R4\_Path\_Dereg\_Req}$.

STEP 2

Anchor ASN-GW sends a *Path_Dereg_Rsp* message to Serving ASN-GW and starts $T_{R4\_Path\_De\text{-}Reg\_Rsp}$. Upon receipt of the *Path_Dereg_Rsp* message, Serving ASN-GW stops timer $T_{R4\_Path\_Dereg\_Req}$.

Serving ASN-GW sends a *Path_Dereg_Rsp* message to BS and starts timer $T_{R6\_Path\_Dereg\_Rsp}$. Upon receipt of the *Path_Dereg_Rsp* message, BS stops timer $T_{R6\_Path\_Dereg\_Req}$.

STEP 3

BS sends a *Path_Dereg_Ack* message to Serving ASN-GW. Upon receipt of the *Path_Dereg_Ack* message, Serving ASN-GW stops timer $T_{R6\_Path\_Dereg\_Rsp}$.

Serving ASN-GW sends a *Path_Dereg_Rsp* message to Anchor ASN-GW. Upon receipt of the *Path_Dereg_Rsp* message, Anchor ASN-GW stops timer $T_{R4\_Path\_Dereg\_Rsp}$.

4.12.4.2 R6 Data Path De-Registration Procedure

The following call flows describe the R6 Data Path De-Registration procedure.

4.12.4.2.1 R6 Data Path De-Registration Procedure Initiated by Anchor ASN-GW

R6 Data Path De-Registration may be initiated by the Anchor ASN-GW.

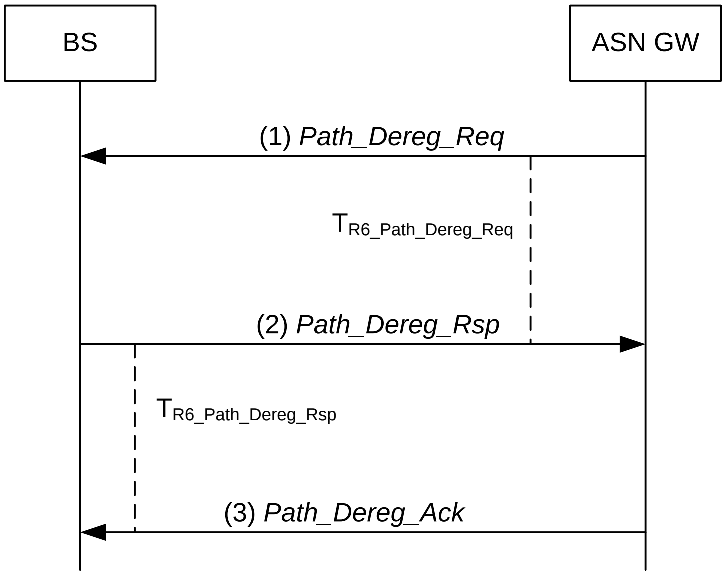


Figure 4-206 – R6 Data Path De-Registration Procedure initiated by Anchor ASN-GW

STEP 1

Anchor ASN-GW initiates Data Path De-Registration procedure by sending a *Path_Dereg_Req* message to BS and starts timer $T_{R6\_Path\_Dereg\_Req}$.

STEP 2

BS sends a *Path_Dereg_Rsp* message to Anchor ASN-GW and starts timer $T_{R6\_Path\_Dereg\_Rsp}$. Upon receipt of the *Path_Dereg_Rsp* message, Anchor ASN-GW stops timer $T_{R6\_Path\_Dereg\_Req}$.

STEP 3

Anchor ASN-GW sends a *Path_Dereg_Ack* message to BS. Upon receipt of the *Path_Dereg_Ack* message, BS stops timer $T_{R6\_Path\_Dereg\_Rsp}$.

4.12.4.2.2 R6 Data Path De-Registration Procedure Initiated by BS

R6 Data Path De-Registration may be initiated by the BS.

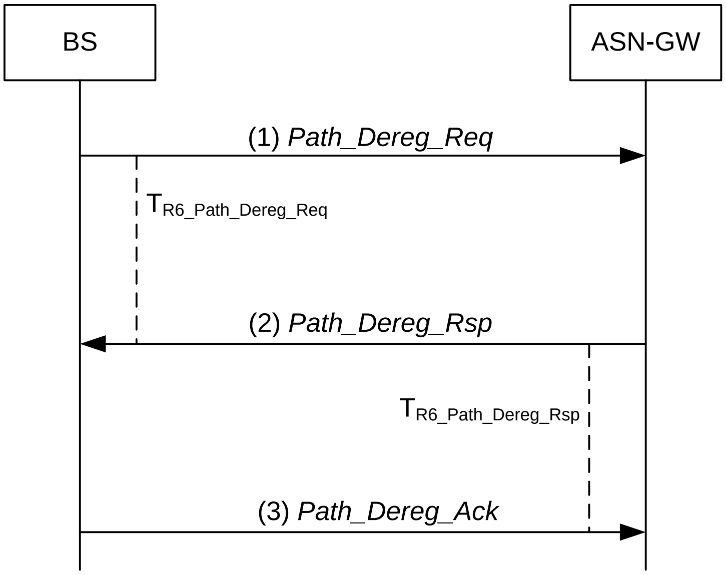


Figure 4-207 – R6 Data Path De-Registration Procedure initiated by BS

STEP 1

BS initiates Data Path De-Registration procedure by sending a *Path_Dereg_Req* message to Anchor ASN-GW and starts timer $T_{R6\_Path\_Dereg\_Req}$.

STEP 2

Anchor ASN-GW sends a *Path_Dereg_Rsp* message to BS and starts timer $T_{R6\_Path\_Dereg\_Rsp}$. Upon receipt of the *Path_Dereg_Rsp* message, BS stops timer $T_{R6\_Path\_Dereg\_Req}$.

STEP 3

BS sends a *Path_Dereg_Rsp* message to Anchor ASN-GW. Upon receipt of the *Path_Dereg_Rsp* message, Anchor ASN-GW stops timer $T_{R6\_Path\_Dereg\_Rsp}$.

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.

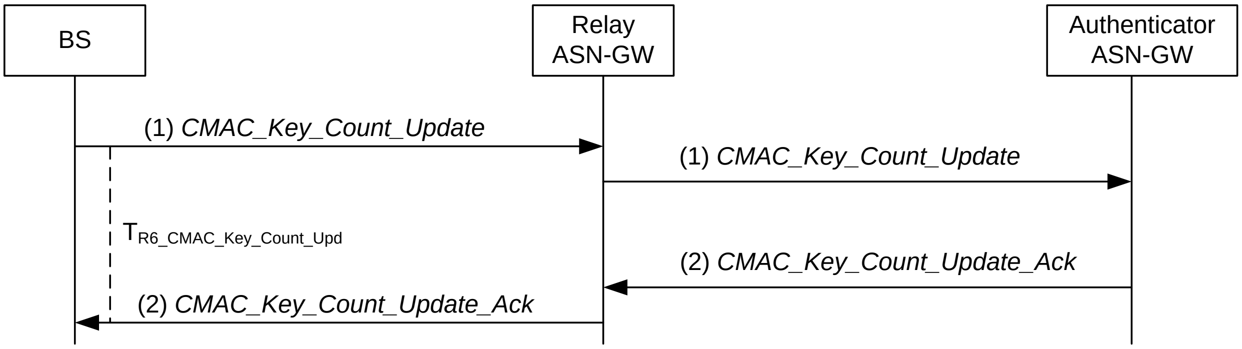

BS
Relay ASN-GW
Authenticator ASN-GW
(1) CMAC_Key_Count_Update
(1) CMAC_Key_Count_Update
T_R6_CMAC_Key_Count_Upd
(2) CMAC_Key_Count_Update_Ack
(2) CMAC_Key_Count_Update_Ack

Figure 4-208 – 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.

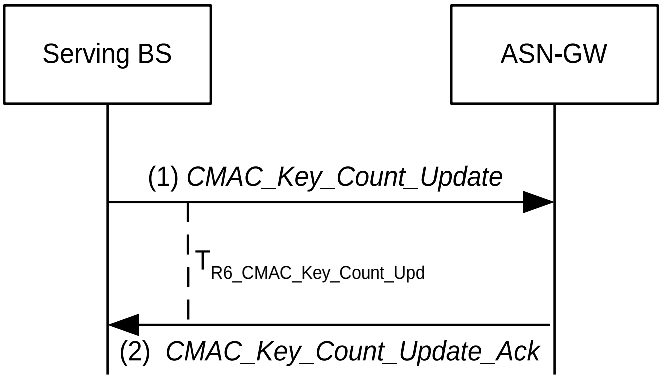


Figure 4-209 – R6 CMAC Key Count Update Procedure

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.

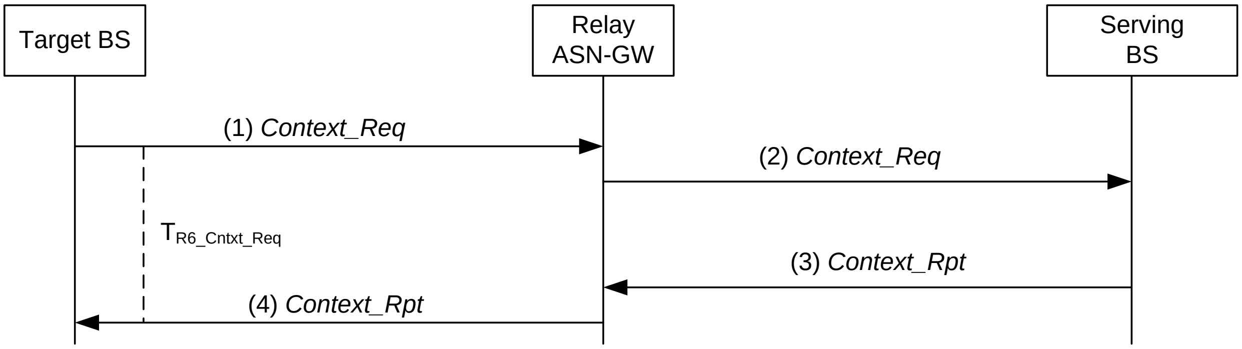


Figure 4-210 – MAC Context Retrieval Procedure

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 $T_{R6\_Cntxt\_Req.}$

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 $T_{R6\_Cntxt\_Req}$.

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.

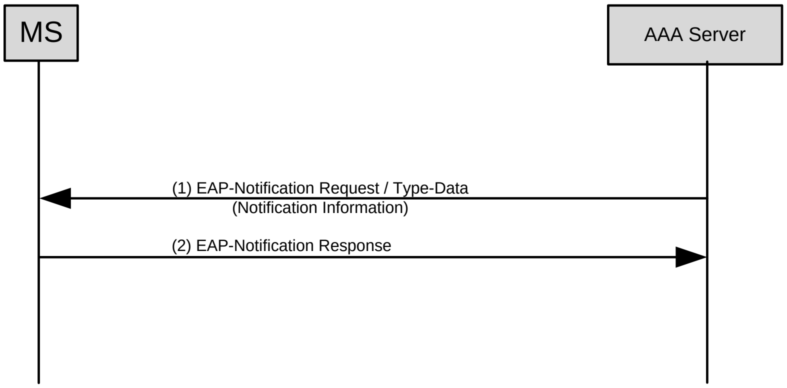

MS
AAA Server
(1) EAP-Notification Request / Type-Data
(Notification Information)
(2) EAP-Notification Response

Figure 4-211 – 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 4-194 – 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[3]
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[4]

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/AMS, ASN and CSN related to establishment and management of MS/AMS' 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/AMS. 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 MS/AMSs 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/AMS. 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/AMS.

4.13.1 AR requirements

Access Router (AR) is the 1st hop IP router for the MS/AMS and is acting as a default gateway for the MS/AMS. 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/AMS NAI and match it with the operator name of the CSN to select the right data path over which the MS/AMS user plane SHALL be delivered to the CSN.

AR SHALL deliver all uplink traffic from the simple IP MS/AMS to the CSN via a data path. When the AR receives an uplink packet from the BS/ABS, it MAY use the GRE key ID of the GRE tunnel over which it received the packet to retrieve the MS/AMS context and then deliver the packet over the data path contained in the MS/AMS context.

AR SHALL receive downlink MS/AMS traffic from the CSN via a data path. AR MAY use the destination IP address of the downlink packet to locate the MS/AMS context. If no matching MS/AMS 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 MS/AMSs using the same IP address. The AR SHALL support MS/AMSs with overlapping private IP addresses and SHALL deliver packets to the appropriate MS/AMS based on corresponding CSN data path which the MS/AMS is associated with.

While in active mode, the AR function handling the MS/AMS traffic cannot be changed or relocated for the duration of the MS/AMS 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/AMS IP address. It intercepts packets destined for the MS/AMS and delivers them to the ASN where the MS/AMS 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/AMS to the ASN where the MS/AMS is attached via the data path.

CR SHALL receive uplink MS/AMS traffic from the ASN where the MS/AMS 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/AMS 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 Visted-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/AMS. 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/AMS 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/AMS Requirements

The MS/AMS 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/AMS, 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/AMS. This is done to prevent MAC address spoofing by a rogue MS/AMS.

In case the DHCP proxy determines that the MS/AMS 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/AMS 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/AMS Identity (Outer-Identity associated with ISF or MAC address) to locate the MS/AMS info in the NAS. If the MS/AMS info contains an MS/AMS address, it will be used to respond back to the MS/AMS with a DHCPOFFER message setting the yiaddr(address) field to the MS/AMS 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/AMS 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/AMS) as follows as default setting:

- T_1 = 0.5 * Lease Time
- T_2 = 0.875 * 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/AMS 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/AMS.

4.13.4.2.2 DHCP Relay requirements

The DHCP relay SHALL handle all DHCP messages sent by the MS/AMS to the broadcast IP address.

The DHCP relay MAY be configured with the DHCP server address during the MS/AMS 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/AMS to the DHCP server.

Upon receiving a DHCPDISCOVER message from the MS/AMS, the DHCP relay SHOULD verify the “chaddr” field in the DHCP header or in the client-identifier option matches the MS/AMS MAC address saved in the MS/AMS session context. This is done to prevent MAC address spoofing by a rogue MS/AMS. 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/AMS context.

If the DHCP relay determines that the MS/AMS 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/AMS context, the DHCP relay MAY consider the following action:

- A rogue MS/AMS 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/AMS. 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/AMS. 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/AMS.

The DHCP relay behavior for handling DHCPREQUEST or DHCPDECLINE from the MS/AMS is same as in the case of DHCPDISCOVER.

When the DHCP relay receives the DHCPREQUEST message from the MS/AMS, it MAY add a relay agent option to the message containing a Subscriber-ID suboption set to the MS/AMS 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/AMS.

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/AMS 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/AMS from the network and the ASN SHALL release all the resources related to the MS/AMS.

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/AMS 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 filed. 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/AMS.

4.13.4.3 FIAA requirements

FIAA MAY be used as one of the address acquisition and network configuration mechanisms between the AMS and the network.

4.13.4.3.1 AMS requirements

The AMS MAY implement and use FIAA for address acquisition obtaining the network configuration parameters. If the FIAA prodcedure is used by the AMS for a given session, other mechanisms (i.e. stateless address autoconfiguration and DHCP) SHOULD NOT be used.

An AMS that wants to use the FIAA procedure SHALL include the Host-Configuration-Capability-Indicator IE set to “1” in the AAI-REG-REQ message it sends to the ABS during the network entry procedure. The AMS SHALL use the configuration parameters it receives (IPv4-Host-Address and/or IPv6-Host-Address, and possibly Additional-Host-Configurations IEs) when sending the AAI-REG-RSP message.

4.13.4.3.2 ABS requirements

The ABS SHALL forward the Host-Configuration-Capability-Indicator and/or Requested-Host-Configurations IE parameters it receives from AMS over AAI-REG-REQ to the ASN-GW over MS_Attachment-Req. Similarly, the ABS SHALL forward the IPv4-Host-Address, IPv6-Host-Address, and Additional-Host-Configurations IEs it receives from ASN-GW over the MS_Attachment_Rsp to the AMS over AAI-REG-RSP.

4.13.4.3.3 AR requirements

When the AR (ASN-GW) receives a *MS_Attachment_Req* message carrying Host-Configuration-Capability-Indicator IE set to “1”, it SHALL respond with *MS_Attachment_Rsp* message carrying IPv4-Host-Address and/or IPv6-Host-Address, and optionally Additional-Host-Configurations IEs. The values carried in these attributes are the ones obtained from the NAS.

When the framed addresses from both VCSN and HCSN are available at the VCSN NAS, it means the HCSN authorized the VCSN to choose the anchoring CSN. Since authorized by the HCSN, the VCSN may decide to anchor the session itself. The details of how the HCSN and/or VCSN decide are outside the scope of this specification. The AR MAY set the subnet option to the value indicated in the Framed-IP-Netmask attribute, in case such attribute is available at the NAS. The AR SHALL set the Subnet option to the value 255.255.255.255 and MAY set the Router option to its own IP address. It SHALL set the Domain Name Server option to the address of the DNS server available at the NAS.

4.13.4.3.4 CR requirements

None.

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/AMS, in accordance with WiMAX Rel 1.0.

4.13.5.1 MS/AMS Requirements

There are no specific requirements on the IPv6 MS/AMS related to the simple IPv6 service. MS/AMS SHALL use either stateless (RFC 4862) or stateful (DHCPv6 [RFC 3315] or FIAA) address configuration mechanisms. Available address configuration mechanisms are subject to the local network policy. MS/AMS is informed about availability of stateless address autoconfiguration and DHCPv6 methods via Router Advertisement message as per RFC 4861 and RFC 4862.

MS/AMS MAY use FIAA or 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/AMS 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/AMS 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/AMS address has expired, it SHALL initiate procedures to tear down the MS/AMS 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/AMS 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/AMS NAI with the domain name of the CSN operator and relay the DHCP messages to the DHCP servers matching the domain of the MS/AMS.

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/AMS.

The DHCP relay MAY detect that the lease time of an address(es) assigned to the MS/AMS has expired. In such case DHCP relay SHALL initiate procedures to tear down the MS/AMS 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/AMS during the MS/AMS 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/AMS, the DHCP server MUST assign an address whose prefix is unique per MS/AMS, as per WiMAX Forum® Network Architecture Rel 1.0 IPv6 link model.

Messages between DHCP relay and DHCP server SHALL be exchanged securely.

4.13.5.3 FIAA requirements

FIAA requirements for Simple IPv6 is same as the requirements for Simple IPv4. See Section 4.13.4.3.

4.13.5.4 AR Requirements

If the AR is configured to enable stateless address autoconfiguration of the MS/AMS address, it SHALL include the MS/AMS 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 MS/AMSs 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/AMS or it MAY have received prefix from the AAA server in the Framed-IPv6-Prefix attribute.

4.13.5.5 CR Requirements

None.

4.14 Simple Ethernet Service Management

This section describes procedures between the MS/AMS, ASN and CSN related to establishment and management of MS/AMS 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/AMS. 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/AMS. 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/AMS requirement

The MS/AMS 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/AMS to the CSN via the data path identifier contained in the MS/AMS context.

L2FW SHALL receive downlink MS/AMS traffic from the CSN via a data path. L2FW SHALL use data path identifier of the downlink packet to locate the MS/AMS context. If no matching MS/AMS context is found, the L2FW SHALL discard the received downlink packet.

While in active mode, the L2FW function handling the MS/AMS traffic can not be relocated for the duration of the MS/AMS 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/AMS Ethernet Service. It intercepts packets destined for the MS/AMS and delivers them to the ASN where the MS/AMS 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/AMS to the ASN where the MS/AMS is attached via the data path.

eCB SHALL receive uplink MS/AMS traffic from the ASN where the MS/AMS 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/AMS being authenticated. In this case the ASN SHALL NOT provide the layer 3 DHCP relay service for this MS/AMS.

The L2 DHCP relay SHALL intercept all DHCP messages sent by the MS/AMS 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/AMS context. The MS/AMS 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/AMS.

Subscriber ID SHALL be set to the Outer-Identity of the MS/AMS.

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/AMS. The DHCP relay SHALL use the Circuit ID suboption to identify the BS/ABS to which the message SHALL be delivered.

DHCP relay SHALL silently discard any DHCPOFFER and DHCPACK messages that are sent by the MS/AMS. 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.

4.14.6 FIAA Requirements

AMS and network SHALL NOT use FIAA when using Ethernet Service.

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 BS/ABSs 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, R1.5, R1.6, and R2.0) 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_i, may involve certain capabilities Cj.
- For proper application of such capability Cj, 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 Cj 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/ABS 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/ABS.

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.

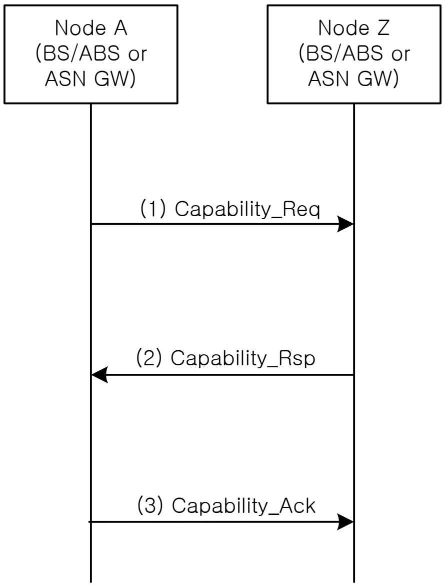


Figure 4-212 – Release/Capability negotiation procedure (push or pull mode)

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 or higher). 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 Cj .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 4-195 – 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	CM	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	M	Indicates which Hot-Lining modes are supported.
>>Support-of-RRM	5.3.2.439	O	To indicate whether RRM is supported or not.

IE	Reference	M/O	Notes
>> Support-of-Packet Flow Operation Policy	5.3.2.460	O	Indicate if the per SF Operation Policy is supported. If this TLV is not presentthe per SF airlink encryption on/off policy is a local implementation policy of the ASN and the sender does not support per-SF airlink encryption policy. Therefore the AAA SHALL NOT provide the per airlink encryption on/off policy for the given SF.
Vendor ID	5.3.2.33	O	24-bit vendor-specific Organization Unique Identifier (OUI) of the Network Element Vendor or Network Provider.
>>Support-of-IPv6	5.3.2.461	O	Indicate whether IPv6 is supported or not.

This message is sent from a network node (say “Node A”, i.e. a BS/ABS 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 4-196 – Capability_Rsp

IE	Reference	M/O	Notes
Failure Indication	5.3.2.426	O	
WiMAX Release Info (one or more)	5.3.2.427	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	5.3.2.428	M	Each WiMAX_Release_Info TLV SHALL include the WiMAX_Release it refers to.
>Capabilities Info	5.3.2.229	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.

IE	Reference	M/O	Notes
>>Capabilities Negotiation Mode	7.3.2.7 of the ROHC Standalone Spec	CM	Indicates the Capabilities Negotiation Mode. The value may be set to: 1 – Complete List of Capabilities 2 – Individual Capabilities
>>ASN-GW ROHC Capability	5.3.2.429	O	To indicate whether ROHC is supported or not.
>>Support-of-MCBCS	5.3.2.430	O	To indicate whether MCBCS is supported or not.
>>Support-of-HO-DI	5.3.2.431	O	To indicate whether HO-DI is supported or not.
>>Support-of-dMAC	5.3.2.432	O	To indicate whether dMAC is supported or not.
>>Support-of-Accounting	5.3.2.433	O	Indicates which accounting modes are supported.
>>Support-of-IMS-ES	5.3.2.434	O	To indicate whether IMS-ES is supported or not.
>>Support-of-PCC-QoS	5.3.2.435	O	To indicate whether PCC-QoS is supported or not.
>>Support-of-EtherServ	5.3.2.436	O	To indicate whether EtherServ is supported or not.
>>Support-of-LBS	5.3.2.437	O	To indicate whether LBS is supported or not.
>>Support-of-FixedNom	5.3.2.438	O	To indicate whether FixedNom is supported or not.
>>Support-of-Hotlining	5.3.2.439	M	Indicates which Hot-Lining modes are supported.
>>Support-of-RRM	5.3.2.460	O	To indicate whether RRM is supported or not.
>> Support-of-Packet Flow Operation Policy	5.3.2.33	O	Indicates a response from the receiving node regarding the support of Packet Flow Operation Policy. The “absence” of this TLV in the response message implies that per SF airlink encryption on/off policy is a local implementation policy of the sending node.
Vendor ID	5.3.2.461	O	24-bit vendor-specific Organization Unique Identifier (OUI) of the Network Element Vendor or Network Provider.
>>Support-of-IPv6	5.3.2.461	O	Indicate whether IPv6 is supported or not.

This message is sent from a network node (say “Node Z”, i.e. a BS/ABS 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 4-197 – Capability_Ack

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	O	
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.
>R4R6R8 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.

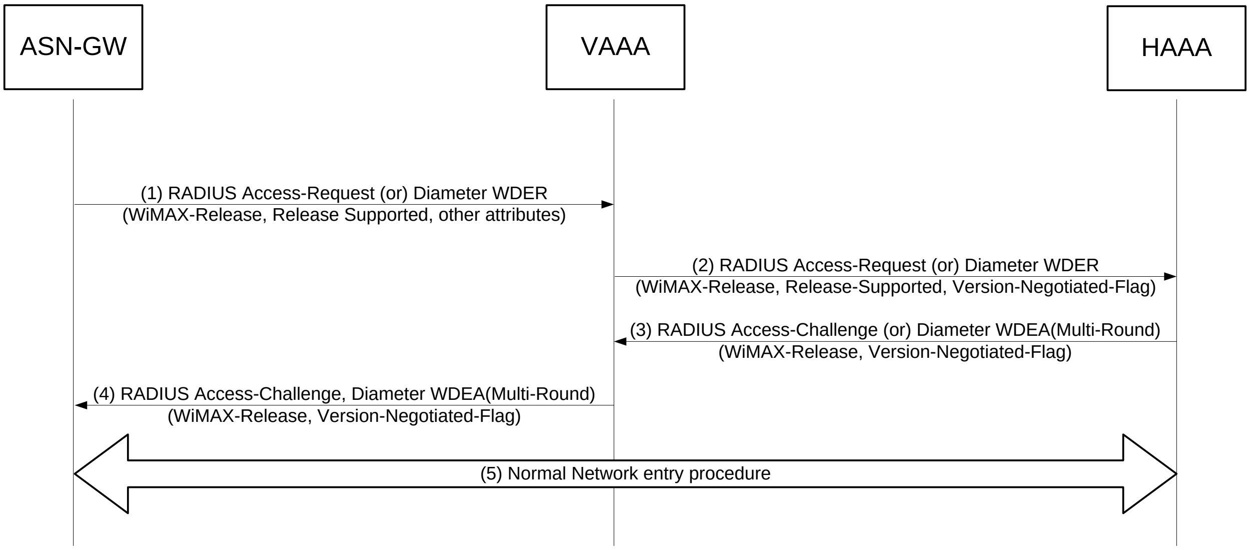

ASN-GW
VAAA
HAAA
(1) RADIUS Access-Request (or) Diameter WDER
(WiMAX-Release, Release Supported, other attributes)
(2) RADIUS Access-Request (or) Diameter WDER
(WiMAX-Release, Release-Supported, Version-Negotiated-Flag)
(3) RADIUS Access-Challenge (or) Diameter WDEA(Multi-Round)
(WiMAX-Release, Version-Negotiated-Flag)
(4) RADIUS Access-Challenge, Diameter WDEA(Multi-Round)
(WiMAX-Release, Version-Negotiated-Flag)
(5) Normal Network entry procedure

Figure 4-213 – Network Entry with R3-R5 Version Negotiation Procedure

STEP 1

During an MS/AMS'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 VNSP. 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 “1.6” 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 WDEA 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.

If the HAAA does not support the release proposed in the WiMAX-Release TLV of the WiMAX-Capability attribute, then the HAAA SHALL set the WiMAX-Release TLV of the WiMAX-Capability attribute to the highest supported release in the Supported-Release TLV of the WiMAX-Capability attribute that it prefers to use. In this case it SHALL set the Version-Negotiation-Flag TLV to three (3) indicating that the AAA Answer message is used for version negotiation.

If the HAAA does not support the proposed version in the WiMAX-Release TLV and the Supported-Release TLV does not contain a release agreeable to by the HAAA, then the HAAA SHALL respond with an AAA Rejection message (in the case of RADIUS Access-Reject packet and in the case of Diameter, WDEA or WHAA with result-code set to indicate failure). The AAA message SHALL indicate the cause of the error by:

- In the case of RADIUS the Error-Cause attribute SHALL be set to "Invalid-Request"(404); and
- In the case of Diameter the Result-Code SHALL be set to "DIAMETER_UNABLE_TO_COMPLY" (5012).

4.16.3 Support for Release 1.0 VAAA

The HAAA is required to detect the presence of a VAAA. The HAAA uses the presence of the NSP-ID set to a different identity than the H-NSP to detect roaming and hence the presence of a VAAA.

In the case of roaming – the HAAA detects the presence of a VAAA - if the Version-Negotiation flag is not present and the WiMAX-Release TLV is not specifying Release 1.0 then the HAAA SHALL negotiation Release 1.0 by setting WiMAX-Release to 1.0 and setting the Version-Negotiation flag to three(3).

The VAAA that complies with release 1.6 is required to add attributes such as the Version-Negotiation-Flag TLV that appears in the WiMAX-Capability attribute.

The VAAA that is compliant with release 1.0 is not required to insert a Version-Negotiation-Flag TLV but is required to ensure an NSP-ID is present in the Access-Request set to the V-NSP identity. If this NSP-ID is not included by the NAS the VAAA SHALL insert this attribute in the Access-Request packet.

The HAAA uses the presence of an NSP-ID set to a different identity than the H-NSP to detect roaming and hence the presence of a VAAA.

4.17 Keep-alive mechanism

The following section describes Keep-alive mechanism between Network Entities (NE) in WiMAX Access Network associated to provide service for the same MS/AMS. This mechanism may be used over R6/ R4 reference points and provides each side with capability to detect failure/ restart of its peer. The NE, detecting the failure/ restart of the peer may take appropriate actions – e.g. clean up the corresponding MS contexts in a “controlled” way.

The Keep-alive mechanism is based on a 2-way transaction (*Keep-alive Req/ Rsp* message exchange). Every NE MAY perform its own independent keep-alive procedure. The trigger for sending *Keep-alive Req* message is out of the specification scope. As an example of one implementation, NE may trigger *Keep-alive Req* to the peer node at the moment it shares MS context with that node. NE MAY continue sending *Keep-alive Req* messages periodically, as long as it shares any MS context with the peer node. Another example is that NE may trigger Keep-alive Req to the peer node at the moment it starts working right after it turns on.

A NE MAY trigger keep-alive transaction to its peer on a periodic basis thus:

- informing its aliveness to the peer and/ or requesting the sign of life from the peer;
- informing a self reboot event of the sending NE and/ or detecting the peer node reboot events since the last keep-alive interrogation.

The NE that supports keep-alive functionality, at the moment of its boot up, SHALL generate the non-zero 32-bit (UTC) timestamp (Last Reset Time) and cache it internally. The NE SHOULD ensure that this value is unique across the multiple restarts of the NE. When sending *Keep-alive Req or Rsp* message, the NE SHALL include this LRT value in the message. This value MAY be interpreted by the keep-alive Receiver to detect the peer‘s restart (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 MS/AMSs, 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.

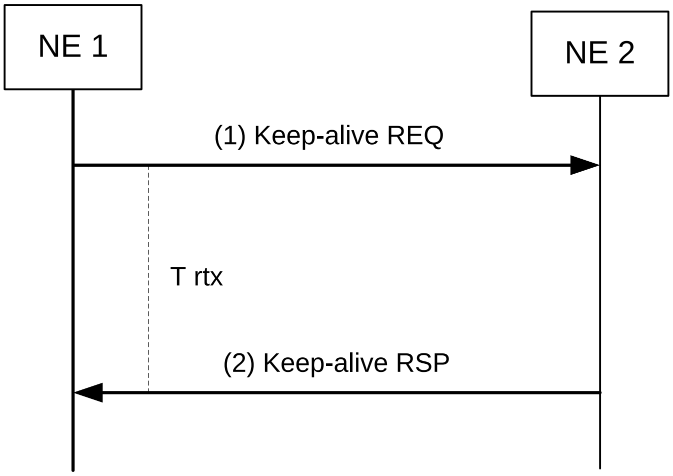


Figure 4-214 – Keep-alive procedure

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 4-198 – 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-octect address) of the reported node.

IE	Reference	M/O	Notes
> 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/AMS sessions and corresponding data paths for MS/AMSs 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 4-199 – 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_{rtx}). 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_{rtx}) 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.

The NE SHALL always include Last Reset Time TLV in the Keep-alive RSP message with the value that was set right after the last boot up.

When the NE receives Keep-alive Req message, it MAY check the received LRT value (the receiver of Keep-alive Req message is not mandated to keep track of the peer that sends the message). If the LRT value received in *Keep-alive Req* message does not match the stored non-zero value for the peer node, the receiver of the message SHALL consider the peer node has passed restart during the time interval from the last keep-alive interrogation. Note that it may take the appropriate action, which is implementation specific.

When NE receives *Keep-alive Req* from the peer it does not maintain any shared contexts for the MS/AMS with, it MAY cache the peer’s IP address/ Identity and its corresponding LRT value.

NE that does not support Keep-alive functionality, SHALL follow error handling procedure as specified in the section 3.4 to signal the sender its inability to support Keep-alive.

4.18 Application Server Discovery

The following describes the procedures on how the MS/AMS discovers the address(es) of Application Server(s) in order to initiate sessions for specific applications. The described procedure is valid for following applications:

- Location Server for the Location Based Service as specified in [LBS-SPEC].

During IP address acquisition at network entry, the MS/AMS/ Application Client MAY send DHCP Request with a DHCP Option [IETF RFC 2132] to acquire the Application Server address(es) or a list of FQDN of the Application Server(s) (AS) for different kind of applications.

If MS/AMS has not requested the Application Server address(es) using DHCP Request during IP address acquisition at network entry, the MS/AMS SHALL send DHCP Inform with a DHCP Option [IETF RFC 2132] to acquire the Application server address(es) or a list of FQDN of the Application Server(s) after IP address acquisition.

If MS/AMS has requested the Application Server address(es) using DHCP Request and obtained the same using DHCP Ack message, then the MS/AMS SHALL NOT send DHCP INFORM with a DHCP Option to obtain Application Server address(es).

4.18.1 DHCP Proxy in the ASN

The NAS MAY receive the address(es) and/or a list of fully qualified domain names (FQDN) of Application Server(s) from the HAAA server during the successful User Access Authentication. The information SHALL be stored in the DHCP Proxy within the ASN.

MS/AMS MAY indicate to the ASN that it wants Application Server address or FQDN list of Application Server in the DHCP Request message during IP address acquisition. Accordingly, the DHCP Proxy MAY optionally include the address(es) of the Application Server(s) in the DHCP Ack.

If the DHCP Inform message from the MS/AMS for the address(es) or a FQDN list of Application Server has been received, the DHCP Proxy SHALL acknowledge the address(es) or a FQDN list of the Application Server(s) by sending the DHCP Ack message to the MS/AMS as defined in RFC 2131 for IPv4 or RFC 3315 for IPv6.

4.18.2 DHCP Relay in the ASN

The MS/AMS MAY indicate to the ASN that it wants Application Server address or FQDN list of Application Server in the DHCP Request message during IP address acquisition. Accordingly, the DHCP Server MAY include the address(es) or FQDN list of the Application Server(s) in the DHCP Ack.

If the DHCP INFORM message from the MS/AMS for the address(es) or a FQDN list of Application Server has been received, the DHCP Relay SHALL relay the message to the DHCP Server. The DHCP Server MAY learn the address or FQDN of Application Server from AAA server.

Upon receiving the acknowledge the address(es) or a FQDN list of the Application Server(s) from the DHCP Server as defined in RFC 2131 for IPv4 or RFC 3315 for IPv6, the DHCP Relay SHALL relay the DHCP ACK message to the MS/AMS.

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/AMS.

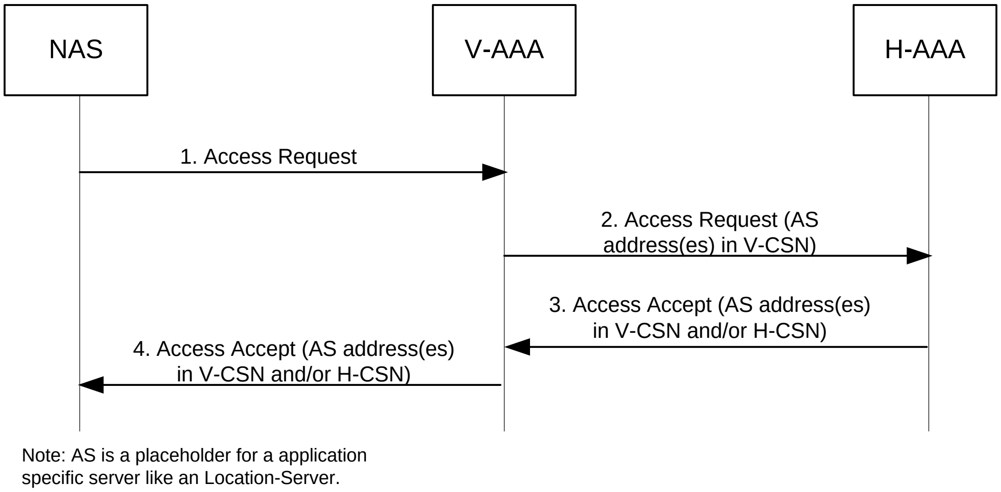

NAS
V-AAA
H-AAA
1. Access Request
2. Access Request (AS address(es) in V-CSN)
3. Access Accept (AS address(es) in V-CSN and/or H-CSN)
4. Access Accept (AS address(es) in V-CSN and/or H-CSN)
Note: AS is a placeholder for a application specific server like an Location-Server.

Figure 4-215 – AS Discovery (Roaming Scenario)

STEP 1

When the NAS gets the access authentication request from the MS/AMS, 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.

4.19 Emergency Telecommunications Service (ETS) Support

4.19.1 Priority Indication

Priority indication in the WiMAX network is expressed in the “Priority Indication” field (the Priority Indication TLV without the subfields is specified Section 11.13.41 of IEEE 802.16 2009 [13]) (a) stored in the QoS parameter set associated with service flows in the Subscription QoS Profile, (b) contained in the compound “QoS Descriptor” parameter of the R3 messages containing service flow information, and (c) contained in the “QoS Parameters” compound parameter of the R6/R4 messages containing the service flow information.

A service flow with a non-zero priority level is called a priority service flow. There is a one-to-one correspondence between Service Flow ID and Transport Connection Identifier (CID) [13] after the service flow is created. The CID associated with a priority service flow is a priority CID. Priority CID can be used as a way to indicate priority in scheduling messages and media with CID information element in the BS.

Note that Priority Indication should be applied before traffic priority.

4.19.1.1 Priority Indication for ETS

The refined structure of the WiMAX Priority Indication field of one byte size [106] is shown in the figure below:

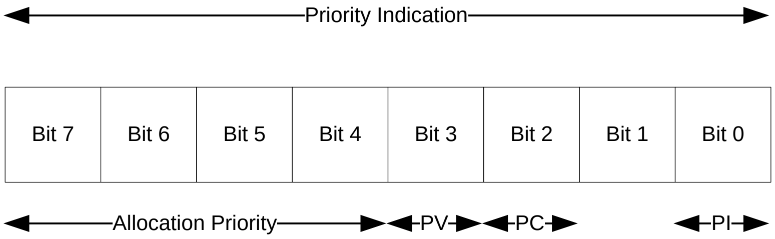


Figure 4-216 – Priority Indication Field

- Bit 0 – Priority Indicator (PI), where value = 1 indicates the priority service is enabled and value = 0 indicates the priority service disabled
- Bit 1 – Un-used
- Bit 2 – Pre-emption Capability (PC), where value = 0 indicates that pre-emption is allowed and value = 1 indicates that pre-emption is not allowed.
- Bit 3 – Pre-emption Vulnerability (PV), where value = 0 indicates that pre-emption is enabled and value = 1 indicates that pre-emption is disabled.
- Bits 4-7 constitute the Allocation Priority sub-field, which provides 15 priority levels/ (values 1 to 15). The value 1 represents represents the highest level of priority. The value 0 is reserved.
  Note that the allocation priority levels can be based on the combination of user priority level and media type.

The 3GPP Allocation Retention Priority (ARP) is a group parameters consisting of three component AVPs [107]: Priority Level, Pre-emption Capability. Pre-emption Vulnerability. The structure size and values are as follows:

	Structure Size	**Values**
Priority Level	32 bit	1 - 15
Pre-emption Capability	32 bit	0, 1
Pre-emption Vulnerability	32 bit	0, 1

In the case of WiMAX – 3GPP PCC interworking [119], the Anchor SFA/BBERF (located with the Anchor Authenticator) shall perform the following mapping between the WiMAX Priority Indication sub-fields and the 3GPP ARP AVPs.

WiMAX Priority Indication Sub-Field	**3GPP ARP AVP**

Allocation Priority	Priority Level
Pre-emption Capability	Pre-emption Capability
Pre-emption Vulnerability	Pre-emption Vulnerability

4.19.1.2 Priority Indication during initial network entry

A Subscription QoS Profile is defined on a per-subscription basis. The subscription is identified by the Network Access Identifier (NAI) that is included in RADIUS or Diameter messages to the Home AAA (H-AAA).

At the time of MS authentication during initial network entry, the H-AAA provides the QoS Descriptor to the ASN Gateway via a RADIUS Access Accept message or a Diameter WiMAX-Diameter-EAP-Answer (WDEA) message. Specifically, the Allocation Priority value in the Priority Indication TLV (contained in QoS Descriptor) of the Initial Service Flow (ISF) associated with the originating MS is passed from the H-AAA to the ASN Gateway, which then passes the Allocation Priority value to the BS through the Path-Reg-Req or Path-Modification-Req message.

4.19.1.3 Priority Indication in ETS Invocation and Revocation in the Non-PCC Architecture

After initial network entry, ETS invocation and the revocation are processed by the AF. The AF passes the Allocation Priority value to the Anchor SFA via the PF/AAA. The interface between the PF/AAA and the AF is not specified in WiMAX Forum® Network Architecture Release 1.5 and 1.6. The Rx interface defined in 3GPP Release 7 [103] can be used as an optional interface between the PF/AAA and the AF for priority indication.

In the case where the Rx interface is used, when an ETS service is invoked or revoked by an authorized ETS User, the AF maps the information related to service type, ETS invoke/revoke signal, and User Level Priority of the ETS User into the corresponding values in Application Identifier and Reservation Priority in the Rx interface.

For session-oriented ETS services (e.g., voice or video telephony), ETS revocation is signaled by service termination. For elastic ETS services (e.g., data transport service) that involve service flows that are still active but without priority after ETS revocation, ETS revocations are explicitly made before service termination.

Upon ETS invocation and revocation, the PF/AAA maps the Application Identifier and Reservation Priority from the AF into Allocation Priority associated with the service flow. The PF/AAA then passes the Allocation Priority information to the Anchor SFA via the QoS Descriptor parameter in a RADIUS Change-of-Authorization message (COA) or in a Diameter WiMAX-Change-of-Authorization-Request (WCAR) message.

When the Anchor SFA receives a RADIUS COA or Diameter WCAR message for ETS invocation or revocation of an active MS, the Anchor SFA SHALL:

1) set the Allocation Priority value in the QoS Descriptor attribute to be the Allocation Priority value in the QoS Parameters of the SF Info structure, and

2) send the RR-Req message with SF Info to the Serving SFA.

When the Serving SFA receives an RR-Req from Anchor SFA to create a new service flow for an ETS request, the Serving SFA forwards the Allocation Priority in SF Info in the Path-Reg-Req message to the Serving BS.

When the Serving SFA receives an RR-Req from Anchor SFA to modify an existing service flow for an ETS request, the Serving SFA forwards the Allocation Priority in SF Info in the Path-Modification-Req message to the Serving BS.

4.19.1.4 Priority Indication in ETS Invocation and Revocation in the PCC Architecture

The interface (PCC-R3-P) of the WiMAX PCC Release 1.6 [108] is based on 3GPP Release 7 Gx interface, which does not contain priority related parameters. This section focuses on the PCC-based priority indication in ETS invocation and revocation in the context of WiMAX-3GPP PCC interworking [119], where the WiMAX ASN Gateway and its Bearer Binding and Event Reporting Function (BBERF) interface with the 3GPP Release 9 PCRF via the Gxa interface [107], and not the PCC-R3-P interface as described in [3].

Note that in 3GPP Release 9 [107], QoS rules can be (a) pre-defined in the WiMAX ASN's BBERF, and activated/de-activated by the PCRF, or (b) dynamically installed, removed, or modified at the WiMAX ASN Gateway/BBERF by the PCRF, through the push mechanism using *Re-Auth-Request* (RAR) and *Re-Auth-Answer* (RAA) or the pull mechanism, using *CC-Request* (CCR) and *CC-Answer* (CCA) messages.

An MPS-Identifier AVP is specified for MPS/ETS for the Rx interface in 3GPP Release 10 PCC [109] but not in 3GPP Rel 8 or 9. Therefore, for 3GPP Release 8 and 9 [110], operator-specific policy, AF-Application-Identifier or just the Reservation-Priority can be used for this purpose prior to deployment of the standardized 3GPP Release 10 PCC solution (see section 6.3 in TS 29.213 [111]).

After initial network entry, ETS invocation and revocation are processed by the 3GPP AF in the network initiated QoS scenario. The AF passes the Reservation-Priority and MPS-Identifier[27] value in a *AA-Request* (AAR) message to the PCRF for establishing/updating the media service flow in the WiMAX ASN. In the 3GPP PCC architecture, the interface between the PCRF and the AF is the Rx interface ([109], [110], [111], [112]) for priority indication.

When an ETS service is invoked or revoked by an authorized ETS User, the AF converts the information related to service type, ETS invoke/revoke signal, and User Level Priority of the ETS User into the corresponding values of MPS-Identifier[27] and Media-Component -Description (including Media-Type and Reservation-Priority) over the Rx interface. The conversion relationship, which depends on the operator policy, is out of scope of this specification.

For session-oriented ETS services (e.g., voice or video telephony), ETS revocation is signaled by service termination. For elastic ETS services (e.g., data transport service) that involve service flows that are still active but without priority after ETS revocation, ETS revocations are explicitly made before service termination.

Upon ETS invocation and revocation the PCRF, based on theMPS-Identifier[27], Reservation-Priority, and Media-Type AVP, provides the related service data flow parameters, including the QoS-Class-Identifier (QCI) and Allocation-Retention-Priority (ARP) values of the related service flows based on the policies. The derivation rules of QCI and ARP in PCRF is defined in [111], [112]. The PCRF then passes the QCI and ARP AVPs in QoS-Rule-Install (for ETS invocation) or QoS-Rule-Remove (for ETS revocation) to the Anchor SFA/BBERF via the Diameter-based Gxa interface.

If more than one service data flows correspond to the requested service type (e.g., ETS data transport service), the PCRF shall change the priority of all of these service data flows via the Gateway Control Session modification procedure and the WiMAX QoS management procedure as described in the following sections.

The Anchor SFA then maps the QCI, ARP, and QoS-Rule-Install/Remove AVPs into the SF info (including QoS Parameters that contains the WiMAX Priority Indication field) and action (create/modify/delete) parameters and sends the mapped parameters in the R4 *RR_Req* message to the Serving SFA as in Sections 7.6.5.2-4 of WiMAX Network Stage 2 Release 1.6 document [113]. The QoS Parameters are then sent from the Serving SFA to the Base Station (BS, which contains the SFM) in R6 *Path_Reg/Dereg/Modification_Req* message, and then from the BS to the MS in the R1 DSA/DSD/DSC message.

When the Anchor SFA receives a RAR message for ETS invocation or revocation of an active MS, the Anchor SFA shall:

1) set the Priority Indication field in the QoS Parameters of the SF Info structure with the ARP value in the QoS rule based on the local policy, and

2) send the *RR_Req* message with SF Info(s) to the Serving SFA.

When the Serving SFA receives an *RR_Req* from Anchor SFA to create a new service flow for an ETS request, the Serving SFA forwards the Priority Indication field in SF Info(s) in the *Path_Reg_Req* message to the Serving BS.

[27] MPS-Identifier is only used in 3GPP Release 10 and above. For 3GPP Release 9 PCC, an operator-specific policy, AF-Application-Identifier or just the Reservation Priority can be used instead of the MPS-Identifier.

When the Serving SFA receives an *RR_Req* from Anchor SFA to modify one or more existing service flows for an ETS request, the Serving SFA forwards the Priority Indication field in SF Info in the *Path_Modification_Req* message to the Serving BS.

In the AMS-initiated QoS scenario, the AMS signals the ETS request via the ranging purpose indicator in R1 AAI-*RNG-REQ* message and the NS/EP service indicator in the R1 *AAI-DSA/DSC-REQ* message [105] to the ABS. The QoS parameters used in the AMS-triggered *DSA/DSC* message can use the QoS profile configured in the AMS as described in Section 7.6.7 of [113]. The ABS forwards the QoS Parameters that include the Priority Indication field to the Serving SFA via the R4 *Path_Reg/Modification_Req*, and then to the Anchor SFA via the *RR_Req* message as described in Sections 7.6.5.5-7 of [113]. The Anchor SFA/BBERF then checks the QoS parameters with its local existing pre-defined PCC rules for pre-provisioned service flows or issues a CCR message with QoS-Information (including requested ARP from the AMS) to the PCRF to generate dynamic PCC rules for dynamic service flows. The PCRF decides the ARP of the IP-CAN bearer based on the requested ARP and ETS user's subscription. If the QoS-Information in the CCA message returned from the PCRF is different from that in the CCR message, the Anchor SFA shall update the QoS parameters to the Serving SFA, the ABS, and the AMS.

The ETS related Gxa parameters include:

A. QoS-Rule-Install

Procedures for the QoS-Rule-Install AVP are specified in Section 5a.3.1 of [107]. This AVP is a group which includes QoS-Rule-Definition AVP and is used to indicate ETS invocation.

B. QoS-Rule-Remove

Procedures for the QoS-Rule-Remove AVP are specified in Section 5a.3.2 of [107]. This AVP is a group which includes QoS-Rule-Definition AVP and is used to indicate ETS revocation.

C. QoS-Rule-Definition

Procedures for the QoS-Rule-Definition AVP are specified in Section 5a.3.3 of [107]. This AVP is a group which includes QoS-Information AVP.

D. QoS-Information

Procedures for the QoS-Information AVP are specified in Section 5.3.16 of [107]. This AVP is group consisting of QoS-Class-Identifier (QCI) AVP and Allocation-Retention-Priority (ARP) AVP.

To support interoperability and interworking with 3GPP EPC, it is recommended that the WiMAX Forum use the same QoS information values as defined in the 3GPP specification [107] for the QCI and ARP.

D.1.1 QoS-Class-Identifier (QCI)

Procedures for the QoS-Class-Identifier AVP are specified in Section 5.3.17 of [107]. Additional QCI characteristics and definitions are specified in section 6.1.7.2 of [114].

D.1.2 Allocation-Retention-Priority (ARP)

Procedures for the Allocation-Retention-Priority AVP are specified in Section 5.3.32 of [107]. This AVP is a group consisting of Priority-Level AVP, Pre-emption-Capability AVP and Pre-emption-Vulnerability AVP. ARP priority level defines the relative importance of a resource request and it is used for admission control in the event of resource limitation such as session establishment or modification. Pre-emption is not required nor supported in the WiMAX ETS, therefore, proper value will be set to inactivate it. Additional ARP characteristics and definitions are specified in section 6.1.7.3 of [114].

D.1.2.1 Priority-Level

Procedures for the Priority-Level AVP are specified in Section 5.3.45 of [107]. The parameter shall be set to a range of value assigned for ETS.

D.1.2.2 Pre-emption-Capability

Procedures for the Priority-Level AVP are specified in Section 5.3.46 of [107]. The parameter is set to “1” for ETS to disable this function.

D.1.2.3 Pre-emption-Vulnerability

Procedures for the Priority-Level AVP are specified in Section 5.3.47 of [107]. The parameter is set to "1" for ETS to disable this function.

The ETS related Rx parameters include:

A. MPS-Identifier AVP

Procedures for the MPS-Identifier AVP are specified in Section 5.3.5 of [109]. It indicates an ETS session.

B. Media-Component-Description AVP

Procedures for the Media-Component-Description AVP are specified in Section 5.3.16 of [109][110]. This AVP is group consisting of Media-Type AVP and Reservation-Priority AVP.

B.1 Media-Type AVP

Procedures for the Media-Type AVP are specified in Section 5.3.19 of [109][110]. It indicates the media type of the services flows.

B.2 Reservation-Priority AVP

Procedures for the Reservation-Priority AVP are specified in [109][110]. The parameter shall include a priority value assigned for the service flows corresponding to the Media-Type.

4.19.1.5 Priority Indication in handover

During the intra-ASN handover, the Allocation Priority values associated with service flows of the MS are maintained when handing over from the Serving BS to the Target BS.

Priority Indication is passed as part of the QoS Parameters in the R6 HO_Req message from the Target ASN Gateway to the Target BS and in the R4 HO_Req message from the Serving ASN Gateway to the Target ASN Gateway.

When a MS is in handover, the Allocation Priority values of all service flows in the MS are used to decide if priority treatment is applied to the handover. Specifically, if and only if the Allocation Priority value of at least one service flow in the MS is non-zero, priority treatment is applied to the handover.

Similarly, during the inter-ASN handover, the Allocation Priority values associated with service flows of the MS are passed from the Serving ASN Gateway to the Target ASN Gateway.

4.19.1.6 Priority Indication in paging by incoming packets for MS in idle mode

When the Anchor SFA/BBERFreceives a COA message or a WCAR message from the PF/AAA (in a non-PCC architecture) or a RAR message from the PCRF (in a PCC architecture) to establish an ETS session to an idle MS, the Anchor SFA SHALL:

1) Set the Allocation Priority value in the QoS parameters field of the SF Info structure associated with the ISF of the terminating MS to be the Allocation Priority value in the QoS Descriptor attribute reflecting the originating user priority level of ETS session, and

2) Send the RR-Req message with SF Info to the Serving SFA of the terminating MS.

The Serving SFA then passes the SF Info parameter (including Allocation Priority) to Anchor DP/FA.

When the Anchor DP/FA in ASN (Y) receives the downlink data to be transmitted to the terminating MS as shown in the figure below (Figure 4-217; Figure 4-177 with call out boxes related to priority indication and treatment), the Anchor DP/FA sends the R4 Initiate_Paging_Request to Anchor PC/LR in ASN (Z) with the Allocation Priority value contained in the SF Info structure. Then the Anchor PC/LR sends the Paging_Announce message with the Allocation Priority value contained in the SF info structure to the applicable PA(s) or Relay PCs in the Paging Group. Each Relay PC forwards the Paging_Announce message to applicable PA(s) in the Paging Group. Then the BS hosting the PA invokes paging priority treatment for the ETS session. In response to priority paging, when the MS enters the network, the BS should recognize the incoming ETS call priority and give the priority treatment to the MS for Idle Mode exit as well as Service Flow addition/change for the ETS call to the terminating MS.

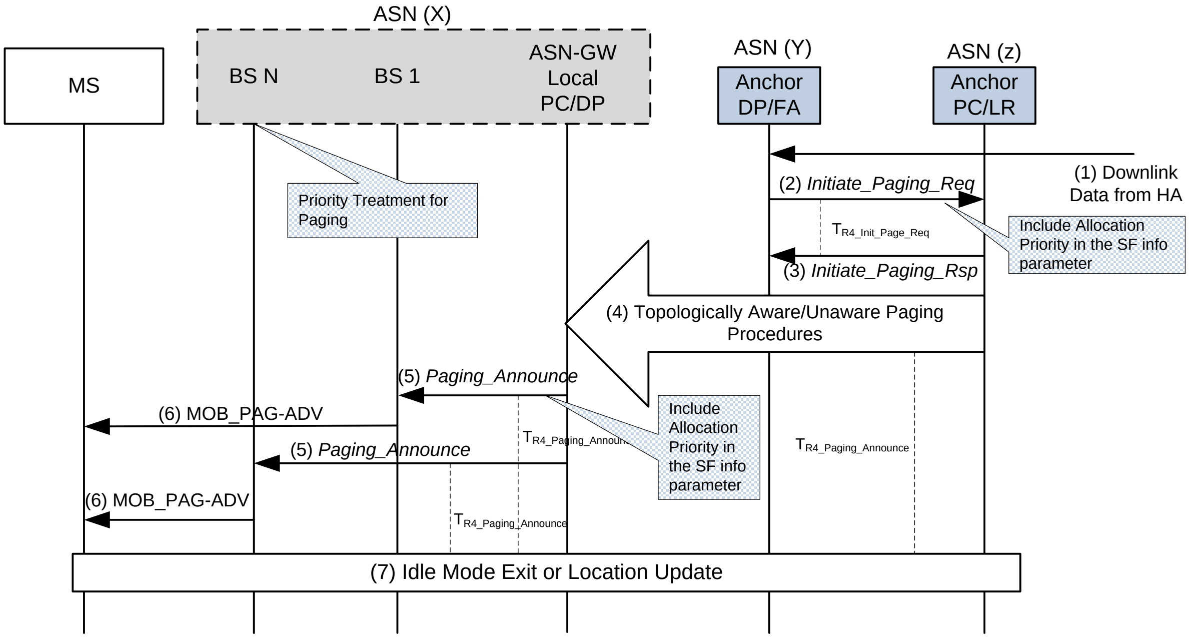


Figure 4-217 – Priority Indication in paging

4.19.1.7 Priority Indication in transporting IP packets

To support ETS, the BS and/or ASN Gateway in the ASN or PF and/or HA/LMA/CR in the CSN FE which transports signaling or user plane IP packets shall provide the flexibility to mark packets associated with ETS with a service provider chosen IP transport marking (e.g., DSCP [104]) that is different from the IP transport marking applied to the non-ETS traffic.

When the BS, ASN Gateway, or HA/LMA/CR participates in the packet transport and can recognize the ETS packets, the WiMAX Network Elements embodying these functions (abbreviated as NEs) shall be able to be configured to give an ETS packet transported through these NEs a higher probability of success during conditions of severe network overload.

Where the BS. ASN Gateway, and HA originate IP packets to be transported and can recognize originated IP packets as ETS packets, these NEs shall mark those IP packets to be transported with a high probability of success during conditions of severe network overload.

4.19.1.8 Priority Indication in USI

The invocation/revocation requests of ETS from the MS get to the Application Server (AS), which in turns triggers priority indication to the AAA or PCRF in the CSN and then to the ASN Gateway and BS in the ASN via either (1) the WiMAX network provided by NSP/NAP or via (2) the WiMAX USI system [115] interfacing with the Internet Application Service Provider (iASP). Sections 4.19.1.4 and 4.19.1.5 address NSP/NAP while this Section addresses USI.

Upon receiving a priority invocation and revocation request for ETS, the iASP issues (a) a createQoSSession Request message to the USI System, which then sends indication of QoS session creation to WiMAX's dynamic QoS subsystem, or (b) a modifyQoSSession Request message to the USI System, which then sends indication of QoS session modification to WiMAX's dynamic QoS subsystem , or (c) a queryQoSSession Request message to the USI System, which then sends indication of QoS session query to WiMAX's dynamic QoS subsystem, and gets back a queryQoSSession Response message for a previously created QoS session.

The above createQoSSession Request, modiftQoSSession Request, and queryQoSSession Response in the U1 interface contains a QoSFlowInfo structure that includes a priority-related parameter, reservationPriority, and a media type parameter, mediaType.

The detailed flows and procedures for createQoSSession, modifyQoSSession, and queryQoSSession are described in Sections 7.5.1.1, 7.5.1.2, and 7.5.1.4 of the Release 1.5 USI specifications [115].

4.19.1.8.1 reservationPriority parameter and mediaType parameter

In Section 10.2.1.9 of the Release 1.5 USI specifications, there is one priority related parameter – reservationPriority. The reservationPriority is of type xsd:int, and is used to assign a priority to the IP flow of the media. Values from 0 to 7 are defined where 0 is the lowest level of priority.

For example, the iASP can assign the ETS request with user priority level = 4 with reseravationPriority value "4".

In Section 10.2.1.9 of the Release 1.5 USI specifications the mediaType is of type xsd:string, and it determines the media type of a session component. The following values are defined: AUDIO, VIDEO, DATA, APPLICATION, CONTROL, TEXT, MESSAGE, OTHER.

For example, the iASP can assign the ETS VoIP service with the media type value "AUDIO" and the ETS data service with the media type "DATA".

The mapping of the values of reservationPriority and mediaType in the U1 interface to the priority indication field in the ASN is performed by the dynamic QoS subsystem.

4.19.1.8.2 Type definition containing the priority parameter

In Section 10.2.2.1 of the Release 1.5 USI specifications [115], the following QoSFlowInfo structure contains the reservationPriority parameter.

Parameter	Type	Occurrence	Description / Clause defined
flowNumber	xsd:int	1	10.2.1.5
flowDescription	FlowDescription	1-2	each for either uplink or downlink flow. In case of bi-directional IP flow, the flowDescription will appear two times. 10.2.2.2
qoSInformation	QoSInformation	1	10.2.2.3
mediaType	xsd:string	0-1	10.2.1.6
codecData	xsd:string	0-1	10.2.1.7
reservationPriority	xsd:int	0-1	10.2.1.9

4.19.1.8.3 Message definitions containing priority parameter for Web services operations

The following three messages contain the QoSFlowInfo type, which includes the reservationPriority parameter.

(1) createQoSSession Request (Section 10.2.3.1.1 of the Release 1.5 USI Specifications)

Parameter	Type	Occurrence	Description / Clause defined
endUserID	xsd:anyURI	0-1	At least one of the user identities (i.e., endUserID and UserIPAddress) SHALL appear. 10.2.1.2
endUserIPAddress	xsd:string	0-1	10.2.1.3
applicationChargingID	xsd:string	0-1	10.2.1.4
qoSFlowInfo	QoSFlowInfo	1+	Every IP flow SHALL contain MS's IP address in its source or destination IP address. 10.2.2.1

(2) modifyQoSSession Request (Section 10.2.3.1.3 of the Release 1.5 USI Specifications)

Parameter	Type	Occurrence	Description / Clause defined
qoSSessionID	xsd:string	1	The identifier generated by the USI server in response to the original QoSSessionCreation operation. 10.2.1.1
qoSFlowInfo	QoSFlowInfo	1+	The IP flows to be modified. The IP flows can be added, removed, or changed. A new flowNumber SHALL be used to add a new QoS IP flow. The IP flows which are not specified but previously provisioned are remained unchanged. 10.2.2.1

(3) queryQoSSession Response (Section 10.2.3.1.8 of the Release 1.5 USI Specifications)

Parameter	Type	Occurrence	Description / Clause defined
result	xsd:Boolean	1	The value TRUE indicates that the USI QoS session is active at the USI server. 10.2.1.10
faultCode	xsd:string	0-1	10.2.1.11
qoSFlowInfo	QoSFlowInfo	0+	does not occur when the result is false 10.2.2.1

4.19.1.9 Priority Indication for SIP

The VoIP service can be implemented in WiMAX based on the WVS [116] or IMS architecture [117] (WVS and IMS are optional in WiMAX) both using the Session Initiation Protocol (SIP) [102] for IP call/session control.

Besides SIP over intra-IMS interfaces that are out of scope of the WiMAX,, SIP priority described in this section is applied to SIP messages on the WiMAX R2 interface between the SS/MS and a WVS Server as well as between the SS/MS and an IMS P-CSCF [118]. The WVS Server and P-CSCF are examples of SIP-capable functional entity (FE).

The SIP priority specifications shown below shall apply to the above SIP-capable FEs in the WiMAX WVS architecture. These specifications can apply to the above SIP-capable FEs in the IMS architecture. However, since IMS development is driven by 3GPP, the applicability of these specifications to the SIP-capable FEs in the IMS architecture may evolve within the 3GPP.

IETF RFC 4412 [102] adds two priority related header fields, namely the Resource-Priority and the Accept-Resource-Priority fields to the SIP headers and fields defined in 3GPP TS 24.229 [117], and specifies the procedures for their usage.

The Resource-Priority header (RPH) field marks a SIP request as desiring prioritized access to resources with the resource values (r-value, in the form of namespace.priorityvalue), i.e., the namespace and associated priority values. The Accept-Resource-Priority header field enumerates the resource values that can be processed.

RFC 4412 specifies two namespaces "ets" and "wps" (emergency telecommunications service and wireless priority service) in support of ETS voice service. Both ets and wps namespaces can support five priority values (0 to 4 with 0 being the highest) that convey levels of importance in the signaling and control layer. Examples of r-value are ets.0, ets.1, ets.2, ets.3, ets.4, wps.0, wps.1, wps.2, wps.3, wps.4, where {ets, wps} are namespaces and {0, 1, 2, 3, 4} are the priority values.

SIP may indicate a request for ETS voice service from the MS via the digits in the Request-URI. Within the WVS or IMS, SIP uses the RPH field to indicate a request for priority network resources. The "ets" namespace in the RPH is used to indicate the ETS call/session and the "wps" namespace is used to indicate the ETS user's priority level. The RPH with the "ets" (and possibly "wps") namespace is part of the SIP INVITE request and other exchanged SIP messages throughout the active phase of the ETS call/session. In the U.S., all ETS voice calls/sessions are assigned the "ets" namespace with the provisioned priority value of "0" while "ets" values of 1 through 4 are reserved for future use. The ETS call/session is recognized by the presence of the "ets" namespace Resource-Priority header value in the SIP message and accorded priority for resource reservation/assignment and priority treatment.

Note that in ETS, the first SIP message from the MS to the AF contains digits and does not have the priority (RPH value = 0). Once the AF recognizes from the digits that it is a priority call, it checks the priority level in the user profile and assign the RPH value accordingly for subsequent SIP messages (e.g., from the originating SIP entities to terminating SIP entities).

4.19.1.10Priority Indication with IEEE 802.16m Air Interface

4.19.1.10.1 NS/EP service flow and ranging purpose indication

In IEEE 802.16m, the AAI system supports National Security/Emergency Preparedness (NS/EP, equivalent to ETS) service flows for designated emergency service personnel.

An AMS can initiate a message over the air with an indication of an NS/EP request, recognized at the AMS, to the ABS. Note that AMS initiated priority indication is different from the network initiated priority indication method described in Release 1.6 where the ETS service request is recognized by the AF in the network and the priority indication is passed from the AF to the CSN, the ASN Gateway, and then the ABS.

During network entry, the AMS may request an NS/EP Service flow setup through initial ranging by setting the Rang¬ing Purpose Indication to code 0b1101 for NS/EP services in the AAI-RNG-REQ message. Upon receiving AAI-RNG-REQ with Ranging Purpose Indication set to code 0b1101, the ABS assigns a NS/EP FID for the NS/EP service flow through the AAI-RNG-RSP.

If the service flow parameters are pre-defined, the AMS transmits the NS/EP message using the Flow ID (FID) for the NS/EP service flow without going through the complete service flow setup through DSA transaction. The ABS grants resources according to the service flow parameters pre-defined for the NS/EP service. If no service flow parameters are pre-defined for the NS/EP service, the AMS and the ABS shall establish the NS/EP service flow via DSA transaction.

During connected state, when no service flow parameters are pre-defined for the NS/EP services, the AMS shall establish the NS/EP service flow using the service flow setup procedure through DSA transaction and raise (set to 1) the NS/EP Indication Parameter in the AAI-DSA-REQ. For the NS/EP service flow, the ABS shall allocate the FID through AAI-DSA-RSP upon receiving the NS/EP service indication in the AAI-DSA-REQ.

When a FID for the NS/EP service flow is allocated in the ABS, the value of the priority indication field associated with the service flow is set or changed depending on whether the associated service flow parameters are pre-defined .

If the parameters of the NS/EP service flow are pre-defined, the value of the priority indication field is set with the pre-defined parameters that contain QoS attributes.

If the parameters of the NS/EP service flow are not pre-defined, the value of the priority indication field is set to the priority value provisioned at the MS if it exists or a default non-zero value otherwise.

4.19.1.10.2 Access Class Priority

The access class value associated with connections maintained in the AMS can be used as a priority indication in contention based bandwidth requests (BR) between an ABS and an AMS over the air. A connection with a higher access class value will have a higher priority to get its BR granted by the ABS to transmit the data.

The access class control procedure described in IEEE 802.16m is as follows:

1. The ABS may advertise a sequence of minimum access classes in the “BR Channel Configuration MIN Access Class” fields within the AAI-SCD (System Configuration Descriptor) for each frame in a superframe, where the “BR Channel Configuration MIN Access Class of the (i+j)-th frame (j = 0, 1, 2, or 3)” field has 2-bits representing 4 integer values {0, 1, 2, 3}. The value of “BR Channel Configuration MIN Access Class” element can be determined by the ABS based on its load condition.
2. This sequence of advertised minimum access classes is maintained in the AMS until another advertisement with the AAI-SCD from the ABS. The AMS also maintains the access class for Transport FIDs assigned to a service flow by the ABS (self initiated or per request of the AMS) established (a) using REG REQ/RSP during the network entry (before authentication) or (b) by DSx exchange post-entry (after authentication). An access class 0, representing the lowest access class, is used for the connections established via (a). The access class value associated with the service flow established via (b) is set by the 2-bit “Access Class” field in the AAI-DSA-REQ or AAI-DSC-REQ message.
3. Based on the sequence of minimum access classes, the AMS can select the frame used for the contention-based random access in order to minimize collision. If no minimum access classes are advertised in the AAI-SCD, then all access classes are allowed. When an AMS has information to send and decides to use the contention-based random access bandwidth request, the AMS shall check if the information the AMS has to send is associated with a service flow whose access class is higher than or equal to the minimum access class advertised by BR channel configuration in the AAI-SCD. If it is not, then the AMS shall wait until the BR channel configuration in the AAI-SCD advertises a sequence of minimum access classes, one of which is less than or equal to the access class of the service flow with data to be sent in the AMS. When the AMS access class is allowed, the AMS shall randomly select a backoff value within the backoff window specified by the access class. This random backoff value indicates the number of BR opportunities that the AMS shall defer before transmitting a bandwidth request.

The access class described above can be viewed as a way to indicate priority between an ABS and an AMS over the air for regular contention-based random access bandwidth requests, where the number of priority level is 4 (with values 0, 1, 2, 3) and the lower value indicates lower priority. The above procedure describes the mechanisms of priority indication and treatment at the ABS and AMS for the R1 interface. An ETS (i.e. NS/EP) service flow can be the assigned with a Transport FID with a higher access class. During congestion,   the minimal access class is broadcast from the ABS to AMSs and the information from the ETS service flows has a higher priority to be sent by the AMSs.

4.19.2 Priority Treatment

Priority treatment in the BS, ASN Gateway, HA/LMA/CR, or signaling priority treatment in the PF or PCRF includes priority resource allocation and priority scheduling/routing based on the priority level expressed in

Allocation Priority associated with service flow passed to these NEs through the above priority indication procedures.

4.19.2.1 Priority Resource Allocation and Priority Scheduling/Routing

Priority resource allocation schemes include (specific implementation is left up to the vendors):

PRA1: admission control for priority service flows: For service flows of the same Schedule-Type (e.g., Best Effort, nrtPS, rtPS, ertPS, UGS), the BS admits the service flow with a high Allocation Priority value with precedence over the service flow with lower Allocation Priority value(s).

PRA2: capacity configuration for ETS services: In support of both ETS and non-priority service load, the BS ensures that a capacity (e.g., a range of 10%-90%) is maintained for non-priority services during overloads and when ETS sessions are active. When the capacity threshold for the public services is configured, but insufficient public service load arrives to fully use the capacity, the residual capacity shall be available to ETS to the extent present. Similarly, if no ETS sessions are active, the public service load can go beyond this capacity threshold.

PRA3: queuing R1 reference point messages related to connection resource allocation: During air interface congestion conditions, the BS queues the R1 reference point messages related to connection resource allocation from ETS but rejects the messages from public services.

Priority scheduling/routing schemes include

PSR1: Priority scheduling for R1 messages and data associated with priority service flows: The BS schedules the uplink and downlink R1 messages and data based on the Allocation Priority value indicated in the associated service flow or the CID (FID for 802.16m) associated with a priority service flow. The R1 messages and data for ETS services are scheduled ahead of those for non-priority services in the BS. Note: on the UL, it will be up to the MS scheduler implementation that is ultimately responsible for allocating the UL bandwidth provided by the BS to the ETS services.

PSR2: Priority routing for IP transport packets: The ASN Gateway and CSN FEs route the IP transport packets for signal and media based on the IP tag (e.g. DSCP) configured for ETS and non-priority services.

In the next section, PRA3 is described in more details since it may affect the flows and timers due to the queuing behavior.

4.19.2.2 Priority treatment on R1 connection resource allocation messages

The PRA3 mechanism can be used in network entry, connection establishment, handover, and paging. The BS performs queue control of R1 connection resource allocation messages for allocating connection resources, such as data transport connections and management connections [13]. The R1 connection resource allocation messages include DSA-REQ, DSC-REQ, RNG-REQ, MOB_PAG-ADV, and MOB_BSHO-REQ, Their related connection resources and procedure are summarized in the table below.

Table 4-200 – Relation of connection resources and procedures for priority treatment on R1

R1 Connection Resource Allocation Message	Connection Resource	Procedure
DSA-REQ	transport connection (serving BS)	service flow addition
DSC-REQ	transport connection (serving BS)	service flow change
RNG-RSP	basic/primary management connection (serving BS)	ranging
MOB_PAG-ADV	paging channel (session terminating BS)	paging

R1 Connection Resource Allocation Message	Connection Resource	Procedure
MOB_BSHO-REQ	transport connection (target BS)	handover

As an example, the service flow addition/change with priority indication and treatment in the successful queuing scenario (i.e. no queue full, no expiry of a timer instance) is illustrated below. The priority indication and treatment steps are shown as the callout boxes in the figure (repeated from Figure 4-76), where priority treatment using priority queuing of R1 connection resource allocation messages is performed at the BS.

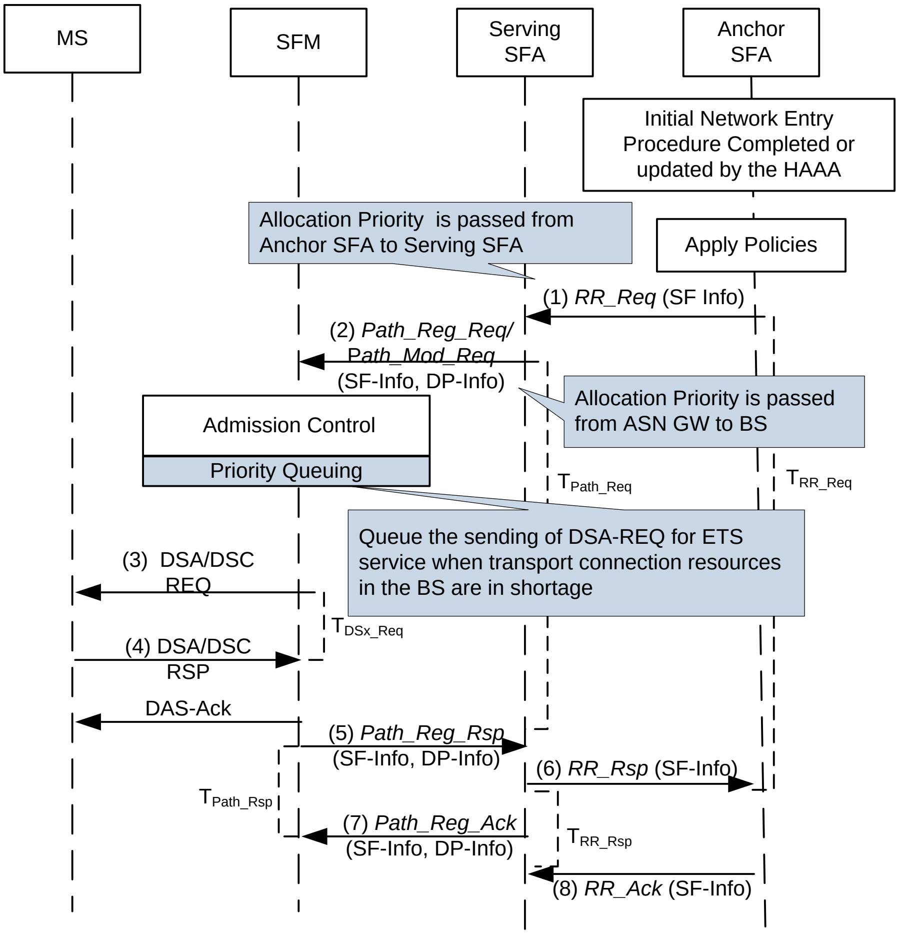

MS
SFM
Serving SFA
Anchor SFA
Initial Network Entry Procedure Completed or updated by the HAAA
Allocation Priority is passed from Anchor SFA to Serving SFA
Apply Policies
(1) RR_Req (SF Info)
(2) Path_Reg_Req/ Path_Mod_Req (SF-Info, DP-Info)
Allocation Priority is passed from ASN GW to BS
Admission Control
Priority Queuing
T_Path_Req
T_RR_Req
Queue the sending of DSA-REQ for ETS service when transport connection resources in the BS are in shortage
(3) DSA/DSC REQ
T_DSx_Req
(4) DSA/DSC RSP
DAS-Ack
(5) Path_Reg_Rsp (SF-Info, DP-Info)
(6) RR_Rsp (SF-Info)
T_Path_Rsp
(7) Path_Reg_Ack (SF-Info, DP-Info)
T_RR_Rsp
(8) RR_Ack (SF-Info)

Figure 4-218 – Service flow addition/change with priority indication

To avoid impacting on the related existing timers, the expiration time for priority timer instance associated with the DSA-REQ and DSC-REQ, MOB_BSHO-REQ, MOB_PAG-ADV, RNG-RSP messages, have the following constraints.

- The expiration time for the priority queue timer instance associated with the DSA-REQ and DSC-REQ messages, should be less than TPath_Req.
- The expiration time for the priority queue timer instance associated with the MOB_BSHO-REQ message should be less than TR6_HO_Rsp.

- ▪ The expiration time for the priority timer instance associated with the MOB_PAG-ADV message should be less than TR6_Paging_Announce.
- ▪ The expiration time for the priority timer instance associated with the RNG-RSP message should be less than TR4_LU_Cnf.

4.19.2.3 ETS Impact on R6/R4/R3 Messages:

For support of ETS, the Priority Indication TLV and QoS parameter TLV are conditionally mandatory, in all messages is present on all R3, R4, and R6 messages containing the QoS-Descriptor TLV or QoS Parameters TLV. These messages and their relevant reference tables are listed below.

Table 4-201 – Relation of connection resources and procedures for priority treatment on R1

Message Name	Reference Table(s)
HO_Req	Table 4-86
HO_Cnf	Table 4-94
HO_Rsp	Table 4-89
Context_Rpt	Table 4-121
Initiate_Paging_Req	Table 4-167
Paging_Announce	Table 4-169, Table 4-170
Path_Reg_Req	Table 4-71, Table 4-72
Path_Reg_Rsp	Table 4-73, Table 4-74
Path_Modification_Req	Table 4-76
Path_Modification_Rsp	Table 4-77
IM_Exit_State_Change_Rsp	Table 4-176, Table 4-179
IM_Entry_State_Change_Req	Table 4-175, Table 4-178
RR_Req	Table 4-63, Table 4-64, Table 4-65, Table 4-66
RR_Rsp	Table 4-68, Table 4-69
RADIUS Access-Accept (AA)	Table 5-20
RADIUS Change-of-Authorization (COA)	Table 5-20
Diameter WiMAX-Diameter-EAP-Answer (WDEA)	Table 5-27, where *[AVP] contains the QoS Parameters TLV as in its corresponding message in RADIUS Access-Accept.
Diameter WiMAX-Change-of-Authorization-Request (WCAR)	Table 5-33, where *[AVP] contains the QoS Parameters TLV as in its corresponding message in RADIUS Change-of-Authorization.

4.19.2.4 Priority Treatment for SIP

For an ETS call/session, priority processing in the signaling and control plane is triggered by the presence of the RPH with the ets namespace, and possibly the wps namespace, in the SIP signaling messages. In addition for an ETS call/session, the WVS or IMS requires priority transport of the signaling messages and priority transport for the user's bearer information (i.e., voice RTP packets). It is expected that for ETS voice the signaling and user bearer can use the same priority transport mechanisms (e.g., DiffServ Code Point, MPLS Label Switched Path) in the WVS or IMS without negatively affecting service performance. Priority transport for the ETS voice signaling provides not only reliable transport of the signaling messages but also, at each SIP-capable FE, facilitates the priority protocol processing (and buffering) of the received signaling messages up the protocol stack to the FE's application processing. This latter capability supports priority processing at each SIP capable FE associated with an ETS call/session, which is important during congestion or overload conditions. An "ETS FE" is a SIP capable FE that has ETS capabilities, including the ability to process the RPH with the "ets" and "wps" namespaces.

The SIP priority procedures for each ETS FE are described in [120].

4.20 Optimized Combined Relocation Procedure

4.20.1 Introduction

This section describes the combined relocation of ASN-GW functions when the Anchor Authenticator and Anchor Data Path Function are co-located in the same ASN-GW.

The Optimized Combined Relocation (OCR) of ASN-GW functions relies on the Authenticator Shifting procedure (i.e. Authenticator Relocation without Re-authentication). Since the Authenticator Shifting procedure doesn't require the re-authentication of the MS/AMS, the Authenticator MAY be relocated without waking up the MS/AMS during the idle mode. When the MS/AMS moves between ASN-GWs across the ASN boundaries while in the idle mode, the ASN-GW functionalities MAY be relocated without waking up the MS/AMS, if allowed by the Operator's policy.

Support for the Optimized Combined Relocation procedure is optional.

4.20.1.1 Requirements

The Optimized Relocation procedures may involve Optimized Combined Relocation of Authenticator, Paging Controller and Anchor DPF or Optimized Standalone Authenticator Relocation. Both sets of procedures require the following ASN-GW and H-AAA behaviors:

1) ASN-GW Requirements

During the Optimized Combined Relocation procedure, it is assumed that the ASN-GW hosts the Authenticator, Paging Controller, and Anchor DPF, and the Authenticator is able to internally communicate with the Anchor DPF within the same ASN-GW.

The ASN-GW that supports the Optimized Relocation procedure SHALL support the *Relocation_Notify*, the *Relocation_Notify_Rsp*, and *Relocation_Trigger* messages with Optimized Relocation Type TLV and related Context Purpose Indicator.

The ASN-GW acting as the old Authenticator SHALL do the following:

- It SHALL create the value of PA_NONCE (nonce1) by setting it to the current value of the CMAC_KEY_COUNT.
- It SHALL be able to generate the Present Authenticator Verification Code, PA_VC, as follows: PA_VC = HMAC-SHA256 ("ocr@wimaxforum.org" | MSK | nonce1 | NAS-ID of New Authenticator)
- It SHALL generate the random 64-bit NA_NONCE (nonce2)
- It SHALL generate the expected value of the New Authenticator Verification Code, xNA_VC, as follows:
  xNA_VC = HMAC-SHA256 ("ocr@wimaxforum.org" | MSK | NA_NONCE)
- It SHALL compare the xNA_VC to the value of the NA_VC received from the ASN-GW acting as the new Authenticator in the *Relocation_Complete_Req* message. If comparison fails, the old

Authenticator SHALL terminate the Optimized Relocation procedure. Otherwise, if comparison succeeds, the old ASN-GW SHALL proceed with relocation of the Authenticator function as described in section 4.20.2 and section 4.21.2.

- It SHALL remove the MSK after the OCR procedure is completed successfully.

The ASN-GW acting as the new Authenticator SHALL be able to do the following:

- It SHALL cache the NA_NONCE (nonce2) received from the old Authenticator in the Relocation_Notify_Rsp message.
- Upon receiving the relocation authorization from the HAAA containing the MSK, it SHALL generate the New Authenticator Verification Code, NA_VC, as follows: NA_VC = HMAC-SHA256 (“ocr@wimaxforum.org” | MSK | NA_NONCE)
- It SHALL include the computed NA-VC in the *Relocation_Complete_Req* message to the old Authenticator as a proof of possession of the MSK.

2) H-AAA Requirements

If the H-AAA supports the Optimized Relocation procedure, the H-AAA MUST have a capability of validating and authorizing the request for authenticator shift including verification of the hash value generated from the present authenticator.

In order to mitigate possible replays of the requests for Optimized Relocations, the HAAA SHALL maintain the 16-bit OCR Counter, OCR_COUNT, for every active MS/AMS session. At the time of successful completion of EAP authentication or re-authentication procedure, the HAAA SHALL reset the OCR_COUNT to ‘1’.

Upon receiving the request for authorizing the Optimized Relocation, the HAAA SHALL compare the received value of the PA_NONCE to the current value of the OCR_COUNT.

If PA_NONCE < OCR_COUNT, the HAAA SHALL reject the relocation. Otherwise, the HAAA SHALL compute the expected value of the Previous Authenticator Verification Code, xPA_VC = HMAC-SHA256 (“ocr@wimaxforum.org” | MSK | nonce1| NAS-ID of New Authenticator ID), and verify that the received PA_VC = xPA_VC.

If the validation is successful, and local policy authorizes relocation from the old Authenticator to the new Authenticator, the H-AAA SHALL send RADIUS *Access-Accept* or Diameter WDEA with the authorization parameters including MSK.

The H-AAA then SHALL set the value of the OCR_COUNT = PA_NONCE.

4.20.1.2 Trigger Conditions

During the idle mode, there are conditions that can trigger the Optimized Combined Relocation initiation by the ASN-GW that supports the OCR procedure (pending the operator’s policy). One example of such trigger is:

Location Update-Triggered

When the MS/AMS moves between ASN-GWs, the MS/AMS detects the change of the Paging Group. As a result, the MS/AMS performs the Location Update procedure. After this procedure, the combined optimization relocation may be initiated.

4.20.2 Procedure Specifications

4.20.2.1 Optimized Combined Relocation in Idle Mode.

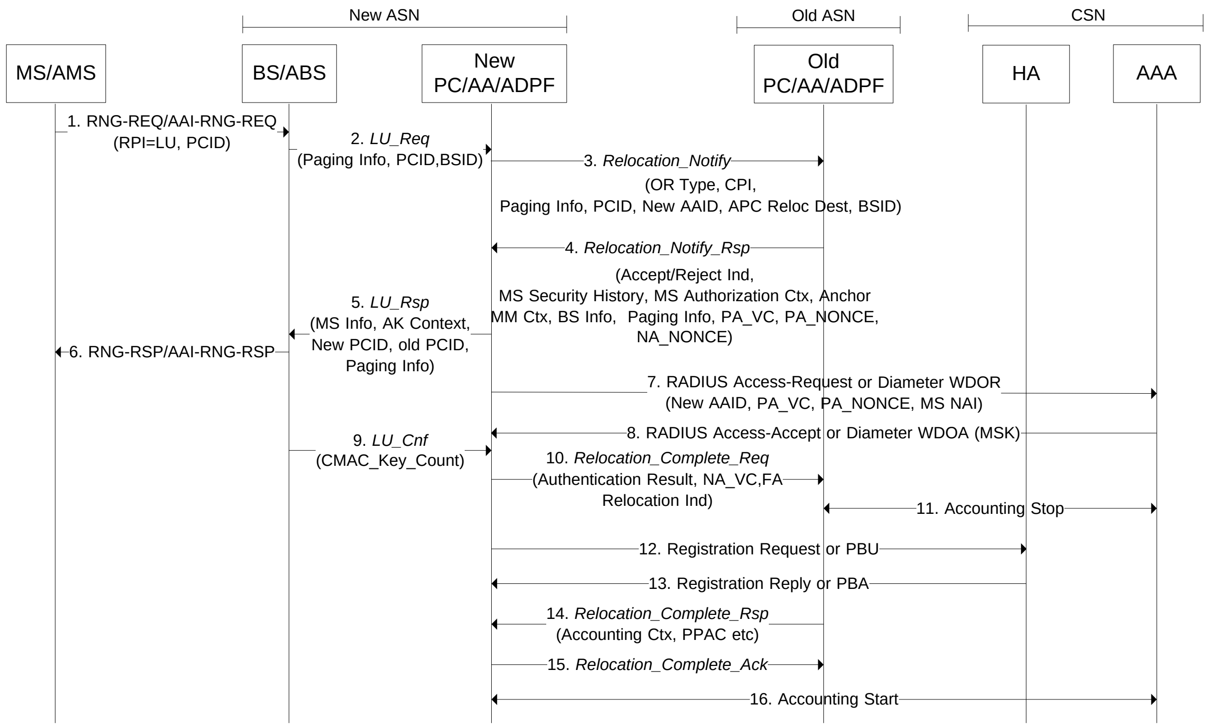

New ASN
Old ASN
CSN
MS/AMS
BS/ABS
New PC/AA/ADPF
Old PC/AA/ADPF
HA
AAA
1. RNG-REQ/AAI-RNG-REQ (RPI=LU, PCID)
2. LU_Req (Paging Info, PCID,BSID)
3. Relocation_Notify (OR Type, CPI, Paging Info, PCID, New AAID, APC Reloc Dest, BSID)
4. Relocation_Notify_Rsp (Accept/Reject Ind, MS Security History, MS Authorization Ctx, Anchor MM Ctx, BS Info, Paging Info, PA_VC, PA_NONCE, NA_NONCE)
5. LU_Rsp (MS Info, AK Context, New PCID, old PCID, Paging Info)
6. RNG-RSP/AAI-RNG-RSP
7. RADIUS Access-Request or Diameter WDOR (New AAID, PA_VC, PA_NONCE, MS NAI)
8. RADIUS Access-Accept or Diameter WDOA (MSK)
9. LU_Cnf (CMAC_Key_Count)
10. Relocation_Complete_Req (Authentication Result, NA_VC,FA Relocation Ind)
11. Accounting Stop
12. Registration Request or PBU
13. Registration Reply or PBA
14. Relocation_Complete_Rsp (Accounting Ctx, PPAC etc)
15. Relocation_Complete_Ack
16. Accounting Start

Figure 4-219 – Optimized Combined Relocation in Idle Mode

STEP 1

MS/AMS sends *RNG-REQ/AAI-RNG-REQ* for Location update request while it is in Idle Mode.

STEP 2

BS/ABS forwards the *LU Request* from MS/AMS, to the new ASN-GW. The *Location Update Req* message will contain the old PCID, and optionally Paging parameters from the MS/AMS and BSID.

In case that the Location Update (LU) message is for AMS, which entered idle mode in the MZone of an ABS, in order for its anchor PC to recognize the AMS' identification, the R6 LU_Req message includes the current PG ID, the current Paging Offset, the current Paging Cycle and the current Deregistration ID TLVs (i.e. combination of the current PGID + the current Paging Offset + the current Paging Cycle + the current Deregistration ID determines uniquely the AMS). In case that the Location Update is for MS/AMS which entered idle mode in BS or LZone of an ABS, the MS/AMS is identified by the MSID value stored in the anchor PC.

STEP 3

Based on operator policy, the New ASN-GW decides to perform the Optimized Combined Relocation. The New ASN-GW sends *Relocation_Notify* to the old ASN-GW to initiate the Optimized Combined Relocation. The message SHALL include the 'Optimized RelocationType' with its value set to 'Idle mode OCR'.

STEP 4

Upon receiving the *Relocation_Notify* with the 'Optimized RelocationType', the old ASN-GW that supports the OCR procedure checks the acceptance of the combined relocation of the local co-location of Paging Controller, Authenticator and Anchor DPF functions. If the old ASN-GW supports OCR and its policy allows the combined relocation, it proceeds with 1) Location Update request from the MS/AMS and 2) Anchor Authenticator relocation and Anchor DPF relocation. If the Location update request from the MS/AMS is valid, the old ASN-GW prepares for the relocation of all three functional entities. For Authenticator relocation, Authenticator in the old ASN-GW sets the CMAC_KEY_COUNT to the current locally maintained value of the CMAC_KEY_COUNT, generates a random value, NA_NONCE (nonce2), and calculates the PA_VC as specified in section 4.20.1.1.If OCR is supported by the old ASN-GW (present Authenticator) then it responds to the new ASN-GW (candidate Authenticator) by sending the *Relocation_Notify_Rsp* with Accept/Rejection code set to the accept value, PA_VC, PA_NONCE (with the value set to CMAC_KEY_COUNT) and NA_NONCE and the required Location Update Response Context including BS Info and Paging Info as well as the required context, for example, MS Security History, MS Authorization Context, Anchor MM Context. Once the old ASN-GW begins an Authenticator relocation procedure it should enter in to a ‘Relocation-Lock’ state avoiding new Relocation process or Reauthentication process initiations until it receives confirmation that Relocation process has been completed - either successfully or not.

If the old ASN-GW doesn’t support the Optimized Combined Relocation, it responds to the new ASN-GW (present Authenticator) by sending the *Relocation_Notify_Rsp* with Accept/Rejection code set to the Reject value and the Failure Indication set to Unsupported Option.

If the authenticator in old ASN-GW is in “reauthentication lock” or “relocation lock” state, the old ASN-GW(Authenticator) SHALL respond to the new ASN-GW which initially requested AA relocation by sending the *Relocation_Notify_Rsp* with Accept/Rejection code. Any further AA relocation/reauthentication request during the Relocation lock state, SHALL be rejected by sending the *Relocation_Notify* set to the Reject value and the Failure Indication set to Locked state.

If the Location update request from MS/AMS is not valid or the old ASN-GW doesn't support the combined relocation, see the error scenarios described below in 4.20.2.1.1. The steps 5-16 below describes a successful scenario.

STEP 5

Upon receiving the *Relocation_Notify_Rsp*, with ‘Location update Status’ tlv set to success, ‘*Anchor PC Relocation Request Response* set to ‘Accept’, ‘Anchor PC ID’ set to new ASN-GW ID, the new ASN-GW becomes the PC for the MS/AMS .The new ASN-GW sends *Location Update Response* to the BS/ABS with Location Update success/fail, New PCID, new paging parameters, MS Info etc.

STEP 6

The BS/ABS sends back the MS/AMS *RNG-RSP/AAI-RNG-RSP* indicating the response of the Location Update request including new PCID and new paging parameters.

STEP 7

Upon receiving the *Relocation_Notify_Rsp* from the old ASN-GW with Accept/Rejection code set to accept value, the new ASN-GW caches the received NA_NONCE value, and sends RADIUS Access-Request or Diameter WDOR to the H-AAA. The *Access-Request* Message includes PA_VC, CMAC_KEY_COUNT and User-Name field set to MS-NAI. Note that this step may happen any time after step 4.

If the received Accept/Rejection code from H-AAA is set to the reject value, the new ASN-GW abandons the combined relocation.

STEP 8

If H-AAA supports the Optimized Combined Relocation procedure, the H-AAA first checks whether the value of the received OCR_COUNT is the same or larger than the internally maintained value of the OCR_COUNT for the MS.

The HAAA then verifies the PA_VC. If the validation is successful, the H-AAA sends RADIUS Access-Accept or Diameter WDOA with the authorization parameters including the MSK and the MN-HA-PMIP4 or MAG-LMA-PMIP6 key with associated SPI value. Note, that the MAG-LMA-PMIP6 is associated with the address of the new Authenticator.

The H-AAA then sets the value of the OCR_COUNT = MAX (PA_NONCE, OCR_COUNT).

If H-AAA fails to verify the PA_VC, it sends RADIUS Access-Reject or Diameter WDOA with Failure Indication. For error scenarios on this see sec 4.20.2.1.1 below.

STEP 9

The BS/ABS sends back the new ASN-GW, Location Update Confirmation including the new CMAC-KEY-COUNT. Note that this message may be received any time after step6, but the new ASN-GW will cache the new value only after step 8.

STEP 10

The new ASN-GW sends the *Relocation_Complete_Req* message to the old ASN-GW (the present Authenticator) to complete the combined relocation. The message includes NA_VC generated by the new Authenticator as described in section 4.20.1.1.

STEP 11

The present Authenticator sends an *Accounting Stop* message so that the H-AAA is aware that the present authenticator is no longer serving the MS/AMS.

STEP 12

The new ASN-GW sends *Registration Request* or PBU to the HA/LMA.

STEP 13

The HA or LMA sends back *Registration Reply* or PBA.

STEP 14

Upon receiving the *Relocation_Complete_Req* message, the present Authenticator (the old ASN-GW in the diagram) verifies the NA_VC and sends back *Relocation_Complete_Rsp*. The message SHALL include Accounting Context and SHALL include PPAQ if this is used.

STEP 15

Upon receiving *Relocation_Complete_Rsp* with Accounting Context and PPAQ, the new ASN-GW sends *Relocation_Complete_Ack* back to old ASN-GW.

Upon receiving *Relocation_Complete_Ack* from the new authenticator, the old authenticator terminates ‘Relocation-Lock’ state.

STEP 16

The new ASN-GW sends *Accounting Start* message so that the H-AAA knows the new Authenticator is now the Serving Anchor Authenticator.

4.20.2.1.1 Optimized Combined Relocation Error Scenarios

Optimized Combined Relocation procedure may fail or be denied in following scenarios:

1. If the Old ASN-GW does not support the optimized combined relocation procedure for PC, Authenticator and ADPF entities, the rejection is indicated in step 4 and all further steps may be abandoned. The New ASN-GW should re-try the Location Update for the MS/AMS as described in section 4.10.2, without invoking the optimized combined relocation procedure.
2. If the Location Update Request of the MS/AMS fails at the Old ASN-GW, the Old ASN-GW SHALL send *Relocation_Notify_Rsp* message with Accept/Rejection code set to the Reject value. The Location Update failure SHALL be indicated by the’ Location update status’ TLV (5.3.2.88).

3. If AAA rejects the Authenticator relocation in step 8, the New Authenticator SHALL notify its failure to the Old Authenticator in step 10 by sending *Relocation_Complete_Req* including Authentication result set to fail. The *Relocation_Complete_Req* SHALL not include FA Relocation indication TLV nor NA_VC. Further steps 11-16 of this procedure should not be performed. Note that the Location Update with PC relocation was successful and MS/AMS has new PCID and new paging parameters. Hence PC relocation is not revoked and MS/AMS is not disturbed.

4. If the AAA rejects the Authenticator relocation in step 8, the *LU_Conf* from the BS/ABS will be terminated at the new (PC) ASN-GW, but CMAC_KEY_COUNT SHALL be send to AA at the Old ASN-GW using the CMAC_Key_Count_Update procedure.

4.20.2.1.2 Message Definitions

The Table 4-202 specifies the Messages and their TLVs which are required for the scenarios.

Table 4-202 – Relocation_Notify from "New" Authenticator to "Old" Authenticator

IE	Reference	M/O	Notes	Applicability
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).	1,2,3
MS Info	5.3.2.103	CM	Contains MS-related context in the nested IEs. This TLV SHALL be included if the message is used for OCR.	1,2,3
>Authenticator ID	5.3.2.19	CM	Indicates the ID of the "new" Authenticator.	1,2,3
>Optimized Relocation (OR) Type	5.3.2.232	CM	Indicates Optimized Relocation Type. This TLV SHALL be included if the message is used for OR.	1,2,3
>FQDN of new NAS Identifier	5.3.2.263	CM	New NAS (New Authenticator) Identifier. The format SHALL be the fully qualified domain name of the new Authenticator. This TLV SHALL be included if the message is used for OR.	1,2,3
BS Info	5.3.2.26	M		1,2,3
> BS ID	5.3.2.25	CM	BS ID indicating the BS where MS /AMS performs location update.	1,2,3
Paging Information	5.3.2.119	M	Paging Information TLV received from MS/AMS.	1,2,3
> Paging Cycle	5.3.2.118	CM		1,2,3
> Paging Offset	5.3.2.120	CM		1,2,3
> Paging Interval length	5.3.2.135	CM		1,2

IE	Reference	M/O	Notes	Applicability
> Paging Group ID	5.3.2.123	CM		1,2,3
> current Paging Cycle	5.3.2.481	CM	Parameter which was assigned to AMS by anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> current Paging Offset	5.3.2.482	CM	Parameter which was assigned to AMS by anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> current Deregistration ID	5.3.2.483	CM	Deregistration ID assigned to AMS by anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
>current Paging Group ID	5.3.2.484	CM	Paging Group ID assigned to AMS by anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> Anchor PC ID	5.3.2.12	CM	Current Anchor PC ID received from MS.	1,2,3
> Anchor PC Relocation destination	5.3.2.13	CM	Identifier for the new Anchor PC for PC relocation.	1,2,3

Table 4-203 – Relocation_Notify_Rsp from “Old” Authenticator to “New” Authenticator

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3
Accept/Reject Indicator	5.3.2.1	M	Indicates Accept/ reject of the corresponding request.	1,2,3
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.	1,2,3
> MSID	5.3.2.102	CM	MSID SHALL be included for the case ONLY for AMS which entered idle mode in MZone of ABS.	3
>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.	1,2,3

IE	Reference	M/O	Notes	Applicability
>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.	1,2,3
> MS Security History	5.3.2.108	M	MS Security history – PMK SN.	1,2,3
>>PMK SN	5.3.2.133	M		1,2,3
>>MS NAI	5.3.2.105	M		1,2,3
>>PMIP-Authenticated-Network-Identity	5.3.2.41	O	Include when assigned by AAA in the RADIUS Access-Accept or the Diameter WDOA. 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.	1,2,3
>>Authorization Policy Support	5.3.2.21	M		1,2,3
>>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.	1,2,3
>> 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.	1,2,3
> MS Authorization Context	5.3.2.100	M	Contains Authorization context parameters of the specific MS.	1,2,3
>>R3 WiMAX Capability	5.3.2.207	M		1,2,3
>>> R3 WiMAX-Release	5.3.2.441	M	WiMAX release negotiated during Initial Network Entry.	1,2,3
>>>R3 Accounting Capabilities	5.3.2.208	M	This TLV SHALL be included if R3 WiMAX-Capability is included in the transmitted message.	1,2,3
>>R3 CUI	5.3.2.210	O		1,2,3
>>R3 Class	5.3.2.211	O		1,2,3
>>R3 Framed IP Address	5.3.2.212	O		1,2,3
>>R3 Framed-IPv6-Prefixs	5.3.2.213	O		1,2,3
>>R3 Visited-Framed-IP-Address	5.3.2.362	O		1,2,3
>>R3 Visited-Framed-IPv6-Prefixs	5.3.2.363	O		1,2,3

IE	Reference	M/O	Notes	Applicability
>>R3 Framed-Interface-Ids	5.3.2.364	O		1,2,3
>>R3 Visited-Framed-Interface-Ids	5.3.2.365	O		1,2,3
>>R3 WiMAX Session ID	5.3.2.214	M		1,2,3
>>R3 Packet Flow Descriptor	5.3.2.215	M		1,2,3
>>>R3 Packet Data Flow ID	5.3.2.216	M		1,2,3
>>>R3 Service Profile ID	5.3.2.218	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Uplink QoS ID	5.3.2.222	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Downlink QoS ID	5.3.2.223	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>SFID	5.3.2.184	M	Associated SFID (one or two).	1,2,3
>>PA_VC (MSKHash1)	5.3.2.233	CM	MSKHash1 is generated by the present Authenticator This TLV SHALL be included if the message is used for OCR.	1,2,3
>>PA_NONCE	5.3.2.234	CM	This TLV SHALL be included if the message is used for OCR. The value SHALL be set to the CMAC_KEY_COUNT.	1,2,3
>>NA_NONCE(nonce2)	5.3.2.235	CM	This TLV SHALL be included if the message is used for OCR.	1,2,3
> REG Context	5.3.2.144	CM	This TLV SHALL be included in case of idle mode OCR.	1,2,3
>>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.	1,2
>>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.	1,2
>>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. It is named as 'CS type support' in 16m.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ARQ is supported).	1,2
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>>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.	1,2
>>>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.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. packing supported).	1,2
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ertPS supported).	1,2
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Multicarrier capabilities	5.3.2.485	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Zone Switch Mode Support	5.3.2.486	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3

IE	Reference	M/O	Notes	Applicability
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Interference mitigation supported	5.3.2.488	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>E-MBS capabilities	5.3.2.489	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Channel BW and Cyclic prefix	5.3.2.490	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>frame configuration to support legacy R1.0	5.3.2.491	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Persistent Allocation support	5.3.2.492	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Group Resource Allocation support	5.3.2.493	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Co-located coexistence capability support	5.3.2.494	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>HO Trigger Metric Support	5.3.2.326	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>EBB Handover support	5.3.2.495	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3

IE	Reference	M/O	Notes	Applicability
>>Capability for sounding antenna switching support	5.3.2.497	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>ROHC support	5.3.2.499	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
> State	5.3.2.355	O	State attribute as received in most recent message from AAA server.	1,2,3
> 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).	1,2,3
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.	1,2,3
>>MIP4 Info	5.3.2.96	M	Mobility context of the MS.	1,2,3
>>>HA IP Address	5.3.2.75	M	IP address of the current HA.	1,2,3
>>>Home Address (HoA)	5.3.2.77	M	Home Address (HoA).	1,2,3
>>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA).	1,2,3
>>>Registration Lifetime	5.3.2.147	M	The remaining Mobile IP registration lifetime (measured in seconds).	1,2,3
Context Purpose Indicator	5.3.2.36	M	Bitmap indicating the required context.	1,2,3
Paging Information	5.3.2.119	M	Paging information that old anchor PC assigned to determine identically the AMS.	3
> current Paging Cycle	5.3.2.481	CM	Parameter which was assigned to AMS by old anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3

IE	Reference	M/O	Notes	Applicability
> current Paging Offset	5.3.2.482	CM	Parameter which was assigned to AMS by old anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> current Deregistration ID	5.3.2.483	CM	Deregistration ID assigned to AMS by old anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
>current Paging Group ID	5.3.2.484	CM	Paging Group ID assigned to AMS by old anchor PC. It SHALL be mandatorily included to identify AMS when AMS entered idle mode in MZone of ABS.	3
> Old Anchor PC ID	5.3.2.113	O	This TLV is included in the event of PC relocation.	1,2,3
> Anchor PC ID	5.3.2.12	O	This TLV is included in the event of PC relocation.	1,2,3
>Anchor PC Relocation Request Response	5.3.2.14	O	“Accept” or “Refuse”. Included only if PC Relocation is requested in R4 *LU_Req*.	1,2,3
>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.	1,2,3
> AK Context	5.3.2.6	O	Security context required for BS/ABS to validate the received *RNG-REQ/AAI-RNG-RSP* message from MS/AMS and respond with *RNG-RSP* signed by a valid CMAC digest/AAI-RNG-RSP encrypted by the primary SA.	1,2,3
>>AK	5.3.2.5	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>AK ID	5.3.2.7	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>AK Lifetime	5.3.2.8	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>AK SN	5.3.2.9	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>>CMAC-KEY-COUNT	5.3.2.34	CM	This TLV SHALL be included if AK Context is included in the transmitted message.	1,2,3
>SBC Context	5.3.2.174	CM	This TLV SHALL be included in case of idle mode OCR.	1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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.	1,2
>>Subscriber Transition Gaps	5.3.2.316	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Maximum Transmit Power	5.3.2.317	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>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.	1,2
>>PKM Flow Control	5.3.2.319	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>Security Negotiation Parameters	5.3.2.321	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>>Authorization Policy Support	5.3.2.21	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>MAC Mode	5.3.2.322	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2
>>>PN Window Size	5.3.2.324	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message.	1,2,3
>>>Size of ICV	5.3.2.502	CM	This TLV SHALL be included if Security negotiation parameters is included in the transmitted message. This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.	3
>>Extended Subheader Capability	5.3.2.325	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>HO Trigger Metric Support	5.3.2.326	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Current Transmit Power	5.3.2.327	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS FFT Sizes	5.3.2.328	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2,3
>>OFDMA SS demodulator	5.3.2.329	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS modulator	5.3.2.330	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>OFDMA SS Permutation support	5.3.2.332	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA SS CINR Measurement Capability	5.3.2.333	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA MAP Capability	5.3.2.338	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>Uplink Control Channel Support	5.3.2.339	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>OFDMA MS CSIT Capability	5.3.2.340	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>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.	1,2
>>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.	1,2
>>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.	1,2
>>OFDMA Parameters Sets	5.3.2.50	CM	This TLV SHALL be included if SBC Context is included in the transmitted message.	1,2
>>CAPABILITY_INDEX	5.3.2.503	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>DEVICE_CLASS	5.3.2.504	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>CLC Request	5.3.2.505	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3

IE	Reference	M/O	Notes	Applicability
>>Long TTI for DL	5.3.2.506	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>UL sounding	5.3.2.507	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>OL Region	5.3.2.508	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>DL resource metric for FFR	5.3.2.509	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Max. Number of streams for SU-MIMO in DL MIMO	5.3.2.510	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	5.3.2.511	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>DL MIMO mode	5.3.2.512	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>feedback support for DL	5.3.2.513	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Subband assignment A-MAP IE support	5.3.2.514	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>DL pilot pattern for MU MIMO	5.3.2.515	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Number of Tx antenna of AMS	5.3.2.516	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	5.3.2.517	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for	3

IE	Reference	M/O	Notes	Applicability
			AMS.	
>>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	5.3.2.518	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>UL pilot pattern for MU MIMO	5.3.2.519	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>UL MIMO mode	5.3.2.520	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Modulation scheme	5.3.2.521	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>UL HARQ buffering capability	5.3.2.522	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>DL HARQ buffering capability	5.3.2.523	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>AMS DL processing capability per sub-frame	5.3.2.524	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>AMS UL processing capability per sub-frame	5.3.2.525	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>FFT size(2048/1024/512)	5.3.2.526	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Authorization policy support	5.3.2.21	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Inter-RAT Operation Mode	5.3.2.527	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Supported Inter-RAT type	5.3.2.528	O	This TLV SHALL be included if the advanced air interface defined	3

IE	Reference	M/O	Notes	Applicability
			by the IEEE802.16m is used for AMS.	
>>MIH Capability Supported	5.3.2.529	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>SF Info	5.3.2.185	CM	This TLV SHALL be included in case of idle mode OCR.	1,2,3
>>SFID	5.3.2.184	CM	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
>>Direction	5.3.2.59	CM	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
>>HARQ Context	5.3.2.453	O	Contains HARQ related information for management connections.	1,2
>>>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.	1,2
>>>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.	1,2
>>>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.	1,2
>>CS Type	5.3.2.39	O	This TLV must be included in the transmitted message for the target ASN to setup flow.	1,2,3
>>ARQ Enable	5.3.2.345	CM	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e. This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
>>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.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>>ARQ_WINDOW_SIZE	5.3.2.346	O	This TLV SHALL be included if sent by the MS during initial network entry.	1,2,3
>>>ARQ_RETRY_TIMEOUT-Transmitter Delay	5.3.2.347	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RETRY_TIMEOUT-Receiver Delay	5.3.2.348	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_BLOCK_LIFETIME	5.3.2.349	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_SYNC_LOSS_TIMEOUT	5.3.2.350	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_DELIVER_IN_ORDER	5.3.2.351	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_RX_PURGE_TIMEOUT	5.3.2.352	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2,3
>>>ARQ_BLOCK_SIZE	5.3.2.353	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>RECEIVER_ARQ_ACK_PROCESSING TIME.	5.3.2.354	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message.	1,2
>>>ARQ_SUB_BLOCK_SIZE	5.3.2.531	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message. This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.	3
>>>ARQ_ERROR_DETECTION_TIMEOUT	5.3.2.534	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message. This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.	3
>>>ARQ_FEEDBACK_POLL_RETRY_TIMEOUT	5.3.2.535	CM	This TLV SHALL be included if ARQ Context is included in the transmitted message. This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used.	3

IE	Reference	M/O	Notes	Applicability
>>CID	5.3.2.29	O		1,2
>>FID	5.3.2.471	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>SAID	5.3.2.169	O		1,2,3
>>Packet Classification Rule / Media Flow Description (one or more)	5.3.2.114	O		1,2,3
>>>Classification Rule Index	5.3.2.30	CM	Index assigned to the Packet Classification Rule.	1,2,3
>>>Classification Rule Priority	5.3.2.32	CM		1,2,3
>>>IP TOS/DSCP Range and Mask	5.3.2.85	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol	5.3.2.138	O	Allowed protocols are: TCP, UDP, ...	1,2,3
>>>IP Source Address and Mask	5.3.2.84	O	See IEEE802.16e for further details.	1,2,3
>>>IP Destination Address and Mask	5.3.2.82	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Source Port Range	5.3.2.140	O	See IEEE802.16e for further details.	1,2,3
>>>Protocol Destination Port Range	5.3.2.139	O	See IEEE802.16e for further details.	1,2,3
>>>Associated PHSI	5.3.2.15	O	See IEEE802.16e for further details.	1,2,3
>>>IPv6 Flow Label	5.3.2.470	O		1,2,3
>>QoS Parameters	5.3.2.141	CM	This TLV SHALL be included if SF Info is included in the transmitted message.	1,2,3
>>> DSCP	5.3.2.409	O	TC bit set to 1.	1,2,3
>>>BE Data Delivery Service	5.3.2.24	O	Set to BE delivery.	1,2,3
>>>>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.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>UGS Data Delivery Service	5.3.2.196	O	Set to UGS delivery service.	1,2,3
>>>>Minimum Reserved	5.3.2.95	O	See IEEE802.16e for further	1,2,3

IE	Reference	M/O	Notes	Applicability
Traffic Rate			details.	
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if UGS Data Delivery Service is included in the transmitted message.	1,2,3
>>>>SDU Size	5.3.2.177	O	Represents the number of bytes in the fixed size SDU.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>NRT-VR Data Delivery Service	5.3.2.111	O	Set to NRT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>> Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>RT-VR Data Delivery Service	5.3.2.165	O	Set to RT-VR delivery service.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if RT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>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.	1,2,3
>>>>Unsolicited Polling Interval	5.3.2.200	O	This TLV SHALL be included for Uplink direction if RT-VR Data	1,2,3

IE	Reference	M/O	Notes	Applicability
			Delivery Service is included in the transmitted message.	
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>ERT-VR Data Delivery Service	5.3.2.64	O	Set to ERT-VR delivery service.	1,2,3
>>>>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.	1,2,3
>>>>Maximum Latency	5.3.2.91	CM	This TLV SHALL be included if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Unsolicited Grant Interval	5.3.2.199	O	This TLV SHALL be included for Uplink direction if ERT-VR Data Delivery Service is included in the transmitted message.	1,2,3
>>>>Maximum Traffic Burst	5.3.2.93	O	AAA MAY Provide this TLV.	1,2,3
>>>>Tolerated Jitter	5.3.2.190	O	Maximum delay variation (jitter) (in milliseconds).	1,2,3
>>>>Maximum Sustained Traffic Rate	5.3.2.92	O	See IEEE802.16e for further details.	1,2,3
>>>>Traffic Priority	5.3.2.193	O	See IEEE802.16e for further details.	1,2,3
>>>>Request/Transmission Policy	5.3.2.150	O	See IEEE802.16e for further details.	1,2,3
>>>Global Service Class Name	5.3.2.74	O	See IEEE802.16e for further details.	1,2,3
>>>Service Class Name	5.3.2.179	O	See IEEE802.16e for further details.	1,2,3
>>>Media Flow Type	5.3.2.94	O		1,2,3
>>>Media Flow Description in SDP Format	5.3.2.228	O		1,2,3
>>>Reduced Resources Code	5.3.2.237	O		1,2,3
>>PHS Rule	5.3.2.127	O		1,2,3
>>>PHSI	5.3.2.125	CM	This TLV SHALL be included if	1,2,3

IE	Reference	M/O	Notes	Applicability
			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.	1,2,3
>>>PHSF	0	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSM	5.3.2.126	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
>>>PHSV	5.3.2.130	CM	This TLV SHALL be included if PHS Rule is included in the transmitted message.	1,2,3
> SA Descriptor (one or more)	5.3.2.170	O		1,2,3
>>SAID	5.3.2.169	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Type	5.3.2.173	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3
>>SA Service Type	5.3.2.172	O	This attribute SHALL be included only when the SA type is Static SA or Dynamic SA.	1,2,3
>>Older TEK Parameters	5.3.2.112	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Older TEK Parameters is included in the transmitted message.	1,2
>>Newer TEK Parameters	5.3.2.110	O	This TLV MAY be included if SA Descriptor is included in the transmitted message.	1,2
>>>PN Counter	5.3.2.136	O	When AES CCM is selected, the	1,2

IE	Reference	M/O	Notes	Applicability
			TLV SHALL be included.	
>>>RxPN Counter	5.3.2.166	O	When AES CCM is selected, the TLV SHALL be included.	1,2
>>>TEK	5.3.2.187	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK SN	5.3.2.189	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>>TEK Lifetime	5.3.2.188	CM	This TLV SHALL be included if Newer TEK Parameters is included in the transmitted message.	1,2
>>Cryptographic Suite	5.3.2.38	CM	This TLV SHALL be included if SA Descriptor is included in the transmitted message.	1,2,3

4.20.2.2 Optimized Combined FA and Authenticator Relocation (Active Mode) - “PULL/PUSH” Mode

FA and Authenticator relocation “pull” mode is considered when:

Serving ASN triggers FA and Authenticator relocation process.

FA and Authenticator relocation “push” mode may be initiated if the old ASN-GW with ADPF/FA and Authenticator functions has the sufficient knowledge of the new Serving ASN-GW to initiate a relocation request.

Figure 4-220 presents FA/Authenticator relocation “pull or push” mode.

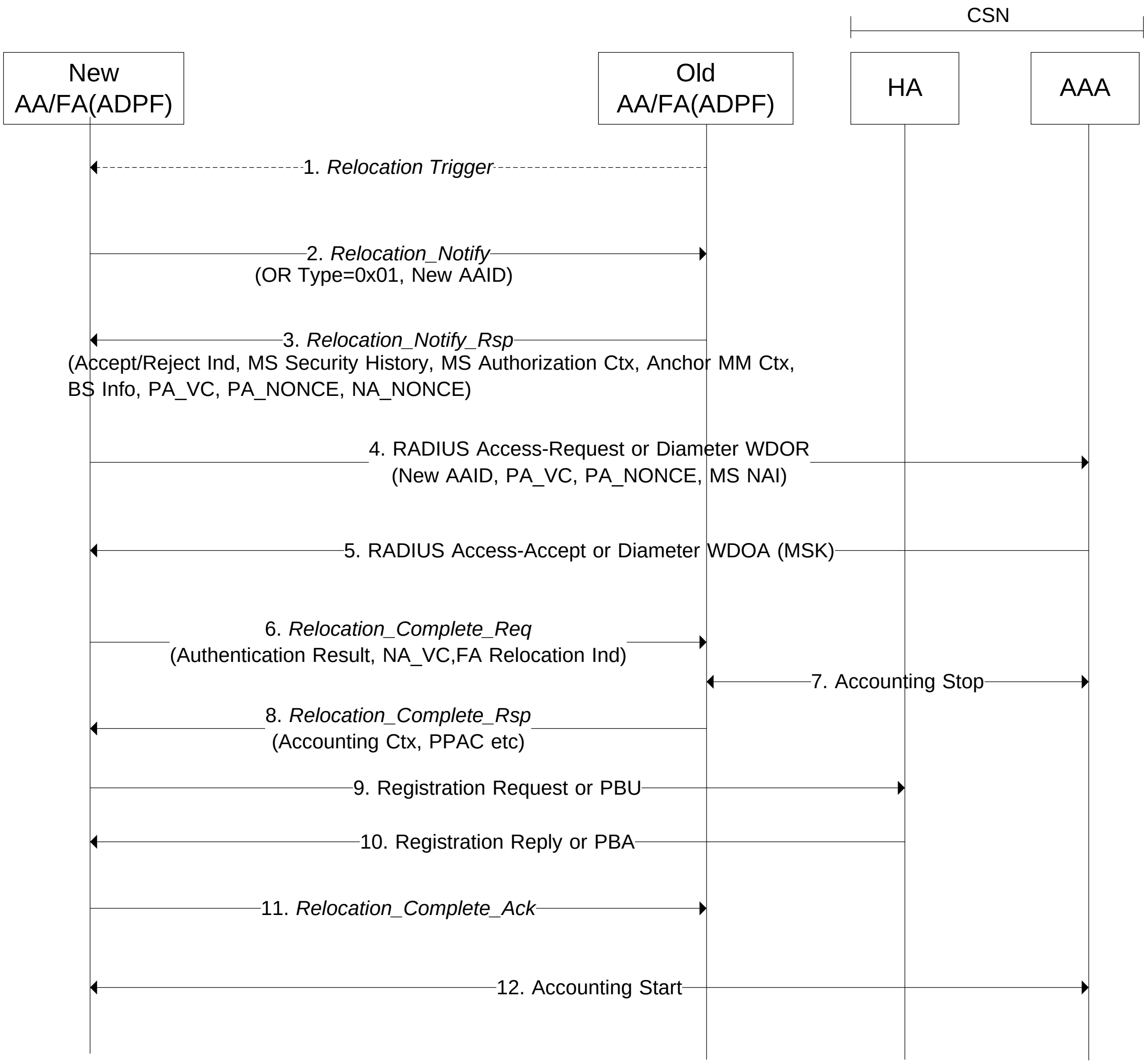

CSN
New AA/FA(ADPF)
Old AA/FA(ADPF)
HA
AAA
1. Relocation Trigger
2. Relocation_Notify
(OR Type=0x01, New AAID)
3. Relocation_Notify_Rsp
(Accept/Reject Ind, MS Security History, MS Authorization Ctx, Anchor MM Ctx, BS Info, PA_VC, PA_NONCE, NA_NONCE)
4. RADIUS Access-Request or Diameter WDOR
(New AAID, PA_VC, PA_NONCE, MS NAI)
5. RADIUS Access-Accept or Diameter WDOA (MSK)
6. Relocation_Complete_Req
(Authentication Result, NA_VC,FA Relocation Ind)
7. Accounting Stop
8. Relocation_Complete_Rsp
(Accounting Ctx, PPAC etc)
9. Registration Request or PBU
10. Registration Reply or PBA
11. Relocation_Complete_Ack
12. Accounting Start

Figure 4-220 – Optimized Combined Authenticator/ADPF Relocation (Active Mode)

STEP 1

If the Old ASN-GW has sufficient knowledge about the new serving ASN-GW, it may on its own initiate the optimized combined relocation of AA and FA, 'PUSH mode' beginning with this step. The Authenticator in the old ASN-GW should enter "relocation lock" state avoiding new Relocation process or Reauthentication process initiations until it receives confirmation that Relocation process has been completed - either successfully or not.

Table 4-204 – Relocation Trigger

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.

IE	Reference	M/O	Notes
> Optimized Relocation (OR Type)	5.3.2.232	CM	Indicates Optimized Relocation This TLV SHALL be included if the message is used for OR.
> Authenticator ID	5.3.2.19	O	Indicates the ID of the 'old' Authenticator GW.

If the new ASN-GW understands the Relocation Trigger message and it supports the proposed 'Active mode OCR', the New ASN-GW proceeds with the following steps as described this section.

STEP 2

The "new" Authenticator/FA sends *Relocation_Notify* message to the "old" Authenticator/FA, thus informing it that Authenticator/FA relocation process starts in the new ASN entity and requesting relevant MS context (e.g., PMK SN). The composition of this message is presented in Table 4-205:

Table 4-205 – Relocation_Notify from "New" Authenticator/FA to "Old" Authenticator/FA

IE	Reference	M/O	Notes
Context Purpose Indicator	5.3.2.36	M	Bitmap indicating the required context. MS Security History SHALL 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	CM	Indicates the ID of the "new" Authenticator.
>FQDN of new NAS Identifier (New AAID)	5.3.2.263	CM	New NAS (New Authenticator) Identifier. The format SHALL be the fully qualified domain name of the new Authenticator. This TLV SHALL be included if the message is used for OCR.
>Optimized Relocation (OR) Type	5.3.2.232	M	Indicates Optimized Relocation Type.

Authenticator/FA ID TLV SHALL be included to indicate the location of the "new" Authenticator/FA. The Anchor MM Context SHALL be requested to perform Authenticator and FA relocation together.

STEP 3

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

The "old" Authenticator/FA responds to the "new" Authenticator/FA with *Relocation_Rsp* message including the requested MS context and Anchor MM Context.

The Authenticator in the old ASN-GW sets the CMAC_KEY_COUNT to the current locally maintained value of the CMAC_KEY_COUNT, generates a random values, NA_NONCE (nonce2), and calculates the PA_VC as specified in section 4.20.1.1.The old Authenticator/FA then responds to the new Authenticator//FA by sending the *Relocation_Notify_Rsp* with Accept/Rejection code set to the accept value, PA_VC, PA_NONCE (set to CMAC_KEY_COUNT) and NA_NONCE.

If the old ASN-GW doesn't support the Optimized Combined Relocation, it responds to the new ASN-GW (Authenticator) by sending the *Relocation_Notify_Rsp* with Accept/Rejection code set to the Reject value and the Failure Indication set to Unsupported Option.

If the authenticator in old ASN-GW is in "reauthentication lock" or "relocation lock" state, the old ASN-GW(Authenticator) SHALL responds to the new ASN-GW which initially requested AA relocation by sending the *Relocation_Notify_Rsp* with Accept/Rejection code. Any further AA relocation/reauthentication request during the Relocation lock state, SHALL be rejected by sending the *Relocation_Notify* set to the Reject value and the Failure Indication set to Locked state.

Table 4-206 – Relocation_Notify_Rsp from "Old" Authenticator to "New" Authenticator

IE	Reference	M/O	Notes	Applicability
Failure Indication	5.3.2.69	O		1,2,3
Accept/Reject Indicator	5.3.2.1	M	Indicates Accept/ reject of the corresponding request.	1,2,3
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.	1,2,3
>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.	1,2,3
>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.	1,2,3
> MS Security History	5.3.2.108	M	MS Security history – PMK SN.	1,2,3
>>PMK SN	5.3.2.133	M		1,2,3
>>MS NAI	5.3.2.105	M		1,2,3
>>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.	1,2,3
>>Authorization Policy Support	5.3.2.21	M		1,2,3

IE	Reference	M/O	Notes	Applicability
>>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.	1,2,3
>> 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.	1,2,3
> MS Authorization Context	5.3.2.100	M	Contains Authorization context parameters of the specific MS.	1,2,3
>>MS NAI	5.3.2.105	M		1,2,3
>>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.	1,2,3
>>R3 WiMAX Capability	5.3.2.207	M		1,2,3
>>> R3 WiMAX-Release	5.3.2.441	M	WiMAX release negotiated during Initial Network Entry.	1,2,3
>>>R3 Accounting Capabilities	5.3.2.208	M	This TLV SHALL be included if R3 WiMAX-Capability is included in the transmitted message.	1,2,3
>>R3 CUI	5.3.2.210	O		1,2,3
>>R3 Class	5.3.2.211	O		1,2,3
>>R3 Framed IP Address	5.3.2.212	O		1,2,3
>>R3 Framed-IPv6-Prefixes	5.3.2.213	O		1,2,3
>>R3 Visited-Framed-IP-Address	5.3.2.362	O		1,2,3
>>R3 Visited-Framed-IPv6-Prefixs	5.3.2.363	O		1,2,3
>>R3 Framed-Interface-Ids	5.3.2.364	O		1,2,3
>>R3 Visited-Framed-Interface-Ids	5.3.2.365	O		1,2,3
>>R3 WiMAX Session ID	5.3.2.214	M		1,2,3
>>R3 Packet Flow Descriptor	5.3.2.215	M		1,2,3
>>>R3 Packet Data Flow ID	5.3.2.216	M		1,2,3
>>>R3 Service Profile ID	5.3.2.218	O	This TLV May be included during Authenticator Relocation.	1,2,3

IE	Reference	M/O	Notes	Applicability
>>>R3 Uplink QoS ID	5.3.2.222	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>R3 Downlink QoS ID	5.3.2.223	O	This TLV May be included during Authenticator Relocation.	1,2,3
>>>SFID	5.3.2.184	M	Associated SFID (one or two).	1,2,3
>>PA_VC (MSKHash1)	5.3.2.233	CM	MSKHash1 is generated by the present Authenticator. This TLV SHALL be included if the message is used for OCR.	1,2,3
>>NA_NONCE(nonce2)	5.3.2.235	CM	This TLV SHALL be included if the message is used for OCR.	1,2,3
>CMAC_KEY_COUNT	5.3.2.34	CM	This TLV SHALL be included if the message is used for OCR.	1,2,3
> REG Context	5.3.2.144	O	Identifies the profile of the capabilities of the registered MS/AMS.	1,2,3
>>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.	1,2
>>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.	1,2
>>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. It is named as 'CS type support' in 16m.	1,2,3
>>Maximum Number of Classifier	5.3.2.291	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>PHS Support	5.3.2.292	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2,3
>>ARQ Support	5.3.2.293	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ARQ is supported).	1,2
>>DSx Flow Control	5.3.2.294	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2

IE	Reference	M/O	Notes	Applicability
>>>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.	1,2
>>>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.	1,2
>>Packing Support	5.3.2.299	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. packing supported).	1,2
>>MAC ertPS Support	5.3.2.300	CM	This TLV SHALL be included if REG Context is included in the transmitted message. For 16m the value may be set by 1(i.e. ertPS supported).	1,2
>>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.	1,2
>>HO Supported	5.3.2.302	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>HO Process Optimization MS Timer	5.3.2.303	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Mobility Features Supported	5.3.2.304	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Sleep Mode Recovery Time	5.3.2.305	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Idle Mode Timeout	5.3.2.268	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>ARQ Ack Type	5.3.2.307	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>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.	1,2
>>MS HO TEK Proc Time	5.3.2.309	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2

IE	Reference	M/O	Notes	Applicability
>>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.	1,2
>>System Resource Retain Timer	5.3.2.311	O		1,2
>>MS Handover Retransmission Timer	5.3.2.312	O		1,2
>>Handover Indication Readiness Timer	5.3.2.313	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>BS Switching Timer	5.3.2.314	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>Power Saving Class Capability	5.3.2.315	CM	This TLV SHALL be included if REG Context is included in the transmitted message.	1,2
>>MAXIMUM_ARQ_BUFFER_SIZE	5.3.2.532	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>MAXIMUM_NON_ARQ_BUFFER_SIZE	5.3.2.533	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Multicarrier capabilities	5.3.2.485	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Zone Switch Mode Support	5.3.2.486	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Capability for supporting A-GPS Method for LBS service	5.3.2.487	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Interference mitigation supported	5.3.2.488	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>E-MBS capabilities	5.3.2.489	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3

IE	Reference	M/O	Notes	Applicability
>>Channel BW and Cyclic prefix	5.3.2.490	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>frame configuration to support legacy R1.0	5.3.2.491	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Persistent Allocation support	5.3.2.492	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Group Resource Allocation support	5.3.2.493	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Co-located coexistence capability support	5.3.2.494	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>HO Trigger Metric Support	5.3.2.326	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>EBB Handover support	5.3.2.495	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Minimal HO Reentry Interleaving Interval	5.3.2.496	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Capability for sounding antenna switching support	5.3.2.497	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>Antenna configuration for sounding antenna switching	5.3.2.498	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
>>ROHC support	5.3.2.499	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3

IE	Reference	M/O	Notes	Applicability
>>AMS initiated aGP Service Adaptation Capability:	5.3.2.500	O	This TLV SHALL be included if the advanced air interface defined by the IEEE802.16m is used for AMS.	3
> State	5.3.2.355	O	State attribute as received in most recent message from AAA server.	1,2,3
> 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).	1,2,3
>>MS Mobility Mode	5.3.2.104	CM	This TLV SHALL be included if Anchor MM Context is included in the transmitted message.	1,2,3
>>MIP4 Info	5.3.2.96	M	Mobility context of the MS.	1,2,3
>>>HA IP Address	5.3.2.75	M	IP address of the current HA.	1,2,3
>>>Home Address (HoA)	5.3.2.77	M	Home Address (HoA).	1,2,3
>>>Care-of Address (CoA)	5.3.2.28	M	Care-of Address (CoA).	1,2,3
>>>Registration Lifetime	5.3.2.147	M	The remaining Mobile IP registration lifetime (measured in seconds).	1,2,3
Context Purpose Indicator	5.3.2.36	M	Bitmap indicating the required context.	1,2,3

STEP 4

Upon receiving the *Relocation_Notify_Rsp* from the old FA/AA with Accept/Rejection code set to accept value, the new FA/AA caches the received NA_NONCE value, and sends RADIUS Access-Request or Diameter WDOR to the H-AAA. The *Access-Request* Message includes PA_VC, CMAC_KEY_COUNT and User-Name field set to MS-NAI.

If the received Accept/Rejection code is set to the reject value, the new FA/AA revokes the combined relocation.

STEP 5

If HAAA supports the Optimized Combined Relocation, the H-AAA first checks whether the value of the received OCR_COUNT is the same or larger than the internally maintained value of the OCR_COUNT.

The HAAA then verifies the PA_VC. If the validation is success, the H-AAA sends RADIUS Access-Accept or Diameter WDOA with the authorization parameters including the MSK and the MN-HA-PMIP4 or MAG-LMA-PMIP6 key with associated SPI value. Note, that the MAG-LMA-PMIP6 is associated with the address of the new Authenticator.

The H-AAA then sets the value of the OCR_COUNT = MAX (PA_NONCE, OCR_COUNT).

If H-AAA fails to verify the PA_VC, it sends RADIUS Access-Reject or Diameter WDOA with Failure Indication. For error scenarios on this see section 4.20.2.1.1 below.

STEP 6

The "new" Authenticator informs the "old" Authenticator about the completion of optimized FA/AA relocation process by sending *Relocation_ Complete_Req* message with Authentication Result, NA_VC, TLVs. 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 4-207:

Table 4-207 – Relocation_Complete_Req Message from "New" Authenticator to "Old" Authenticator

IE	Referenc e	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.
>FA Relocation Indication	5.3.2.71	O	Indicates the FA/AA relocation process. It SHALL be set to indicate "Success" if FA/AA relocation has been Successfully completed with authenticator relocation. Otherwise it should indicate "Failure".
> NA_VC (MSKHash2)	5.3.2.239	M	Contains the hash value of the new authenticator MSKhash2=HMAC-SHA256("ocr@wimaxforum.org" | MSK | NONCE2)

STEP 7

Upon receiving the *Relocation_Complete_Req* message, the present Authenticator (the old ASN-GW in the diagram) verifies the NA_VC and if successful, sends Accounting Stop message so that the H-AAA knows the present authenticator is no longer the serving Authenticator for the MS.

STEP 8

After sending Accounting stop message to AAA, the present Authenticator (the old ASN-GW in the diagram) sends back *Relocation_Complete_Rsp* to new ASN-GW. The message may include Accounting Context and PPAQ. It deletes MS Security context and keys.

The composition of *Relocation_Complete_Rsp* message is presented in Table 4-208:

Table 4-208 – 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).

IE	Reference	M/O	Notes
>>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 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.

IE	Reference	M/O	Notes
>>>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	CM	Associated SFID (one or two). This TLV SHALL be included if R3 Packet Flow Descriptor is included in the transmitted message.
Accounting Context	5.3.2.204	O	Accounting Context.
>Accounting Mode Provisioning	5.3.2.343	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 message.
>>>Time of Day Tariff Switch Offset	5.3.2.255	CM	The time of day time zone 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.

IE	Reference	M/O	Notes
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 9

The new ASN-GW sends *Registration Request* or PBU to the HA/LMA to change HA binding.

STEP 10

The HA or LMA sends back *Registration Reply* or PBA.

STEP 11

Upon receiving *Relocation_Complete_Rsp* with Accounting Context and PPAQ, the new ASN-GW sends *Relocation_Complete_Ack* back to old ASN-GW.

Table 4-209 – Relocation_Complete_Ack

IE	Reference	M/O	Notes
Failure Indication	5.3.2.69	M	Success/Failure indication of the Optimized Combined Relocation procedure.

Upon receiving *Relocation_Complete_Ack* from the new authenticator, the “old” authenticator terminates “relocation lock” state. The “old” Authenticator receiving *Relocation_Complete_Ack* message may proceed with MS context deletion.

STEP 12

The new ASN-GW sends *Accounting Start* message so that the H-AAA knows the new Authenticator is now the Anchor Authenticator.

4.20.2.2.1 Combined AA/FA Relocation Error Scenarios:

Combined Relocation procedure may fail or be denied in following scenarios.

1. If the Old ASN-GW does not support the combined relocation procedure for Authenticator and ADPF entities, the rejection is indicated in step 3 and all further steps may be abandoned. The New ASN-GW should re-try the relocation of FA and AA separately.
2. If the Old ASN-GW initiates a PUSH mode relocation and if the new ASN-GW is not ready to relocate ADPF and AA to itself, the relocation will fail and the new ASN-GW will indicate the failure of the relocation with *Relocation_Complete_Ack* with Failure Indication (similar to 11, but immediately after step 3).
3. If AAA rejects the Authenticator relocation in step 5, Authenticator relocation SHALL be revoked in step 6 by sending *Relocation_Complete_Req* including Authentication result set to fail, FA Relocation indication set to null. Further steps 7-12 of this procedure should be abandoned.

The Old ASN-GW proposes ‘Active mode Optimized Combined Relocation’ with OR Type set to 0x01.

Upon receiving the Relocation Trigger message, the New ASN-GW can behave as follows:

1) If the new ASN-GW doesn't understand the Relocation Trigger message, it silently discards the message. Note that the old ASN-GW may re-try the active mode OCR. It is implementation-specific how many times it retries.

2) If the new ASN-GW understands the Relocation Trigger message but it doesn't support the proposed 'Active mode OCR' but alternatively supports 'Optimized Standalone Authenticator Relocation' , the New ASN-GW may proceed with the steps described in the section 4.21.2.1 'Optimized Standalone Authenticator Relocation'.

3) If the new ASN-GW understands the Relocation Trigger message, but it if it decides to relocate the Authenticator with reauthentication of the MS/AMS, then it may proceed with the steps described in the unoptimized authenticator relocation procedure described in section 4.4.1.5.5.2.

4.21 Optimized Standalone Authenticator Relocation Procedure

4.21.1 Introduction

This section describes the optimized standalone authenticator relocation procedure in case where the MS/AMS re-authentication is not needed at the moment of authenticator shifting.

4.21.1.1 Requirement

The same as 4.20.1.1.

4.21.2 Procedure Specifications

4.21.2.1 Standalone Authenticator Relocation Scenario

Based on operator Policy, the old authenticator may initiate the authenticator Relocation procedure (i.e. Push Mode Standalone Authenticator Relocation). How the old authenticator choose a new Authenticator is out of scope. In this case, the old authenticator sends the Relocation_Trigger message to the new authenticator, which may include some relevant MS context (e.g., PMK SN) in this message.

The Standalone Authenticator Relocation Scenario may also be initiated by the new Authenticator (i.e. Pull Mode Standalone Authenticator Relocation) too.

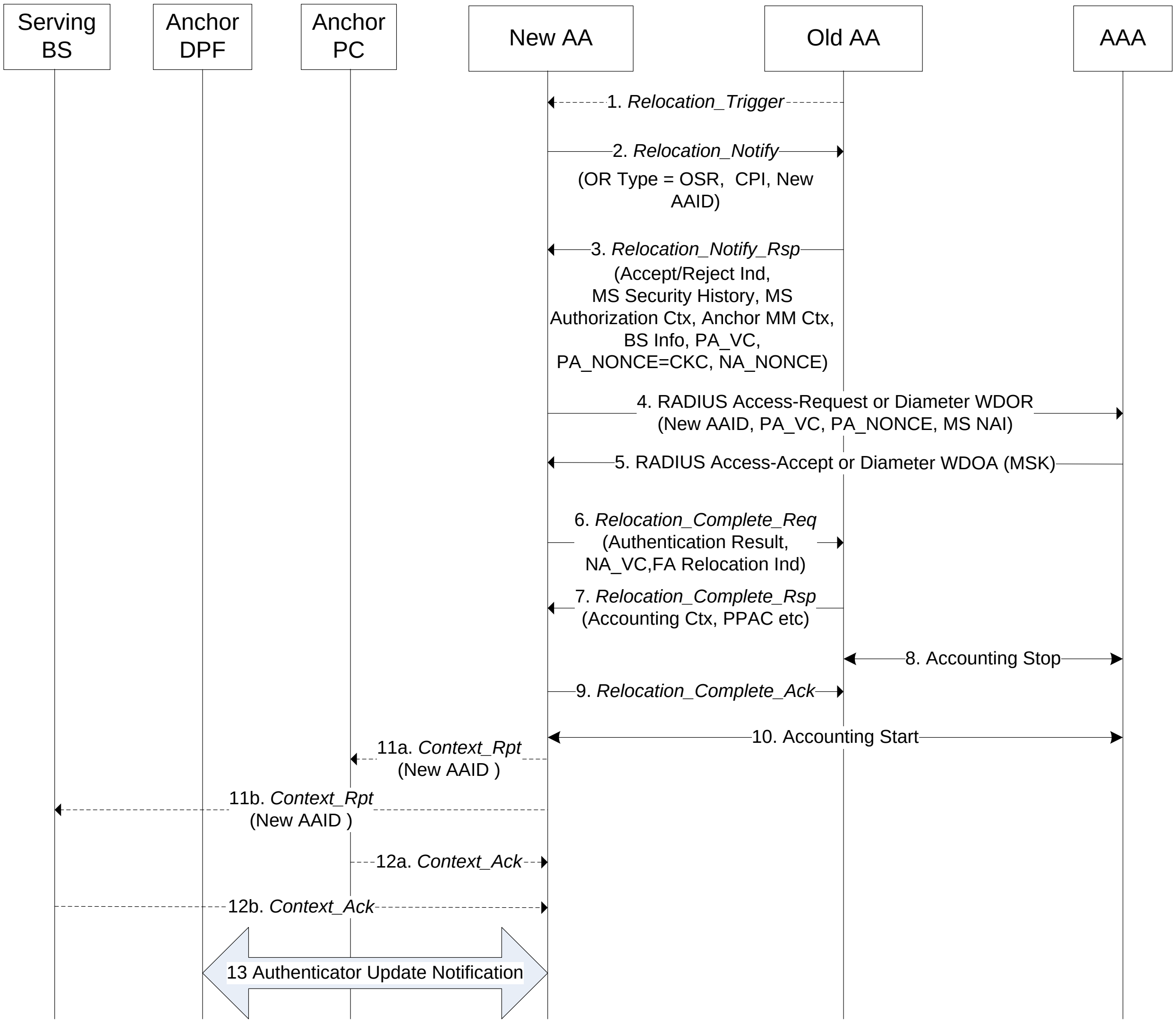

Serving BS
Anchor DPF
Anchor PC
New AA
Old AA
AAA
1. Relocation_Trigger
2. Relocation_Notify
(OR Type = OSR, CPI, New AAID)
3. Relocation_Notify_Rsp
(Accept/Reject Ind, MS Security History, MS Authorization Ctx, Anchor MM Ctx, BS Info, PA_VC, PA_NONCE=CKC, NA_NONCE)
4. RADIUS Access-Request or Diameter WDOR
(New AAID, PA_VC, PA_NONCE, MS NAI)
5. RADIUS Access-Accept or Diameter WDOA (MSK)
6. Relocation_Complete_Req
(Authentication Result, NA_VC,FA Relocation Ind)
7. Relocation_Complete_Rsp
(Accounting Ctx, PPAC etc)
8. Accounting Stop
9. Relocation_Complete_Ack
10. Accounting Start
11a. Context_Rpt
(New AAID)
11b. Context_Rpt
(New AAID)
12a. Context_Ack
12b. Context_Ack
13 Authenticator Update Notification

Figure 4-221 – Standalone Authentication Relocation triggered by the New Authenticator

STEP 1

Based on operator policy, the Old ASN-GW decides to perform the standalone authenticator relocation. The Old ASN-GW sends *Relocation_Trigger* to the New ASN-GW to initiate standalone authenticator relocation (i.e. Push Mode Standalone Authenticator Relocation). The message SHALL include the Optimized Relocation with value 0x02, and optional Authenticator ID for the old Authenticator in this message. The Authenticator in the old ASN-GW should enter “relocation lock” state avoiding new Relocation process or Reauthentication process initiations until it receives confirmation that Relocation process has been completed - either successfully or not. This step is only valid for push mode standalone authenticator relocation.

If the new ASN-GW understands the *Relocation_Trigger* message and it supports the proposed OR Type, the New ASN-GW proceeds with the following steps as described this section.

STEP 2

Based on operator policy, the new serving ASN-GW decides to perform the standalone authenticator relocation (i.e. Pull Mode Standalone Authenticator Relocation). The New ASN-GW sends *Relocation_Notify* to the old ASN-GW to initiate the standalone authenticator relocation. The message SHALL include the Optimized Relocation.

For push mode, if the new ASN-GW does not support the standalone authenticator relocation, it responds it by sending the *Relocation_ Notify* with Accept/Rejection code set to the Reject value and the Failure Indication set to Unsupported Options (Push Mode Standalone Authenticator Relocation).

STEP 3

The authenticator in the old ASN-GW sets the CMAC_KEY_COUNT to the current locally maintained value of the CMAC_KEY_COUNT, generates a random value, NA_NONCE (nonce2), and calculates the PA_VC as specified in section 4.20.1.1. The old ASN-GW (Authenticator) then responds to the new ASN-GW (Authenticator) by sending the *Relocation_Notify_Rsp* with Accept/Rejection code set to the accept value, PA_VC, CMAC_KEY_COUNT and NA_NONCE and the required context, for example, MS Security History, MS Authorization Context, Anchor MM Context. The Anchor PC ID may be included in the Relocation_Notify_Rsp message (Note 1).

Additional for push mode, if the old ASN-GW supports standalone authentication relocation and its policy allows the standalone relocation, the Authenticator in the old ASN-GW should enter "relocation lock" state avoiding new Relocation process or Reauthentication process initiations until it receives confirmation that Relocation process has been completed - either successfully or not. If the old ASN-GW doesn't support the standalone authenticator Relocation, it responds to the new ASN-GW (Authenticator) by sending the *Relocation_Notify_Rsp* with Accept/Rejection code set to the Reject value and the Failure Indication set to Unsupported Option.

If the authenticator in old ASN-GW is in "reauthentication lock" or "relocation lock" state, the old ASN-GW(Authenticator) SHALL responds to the new ASN-GW which initially requested AA relocation by sending the *Relocation_Notify_Rsp* with Accept/Rejection code. Any further AA relocation/reauthentication request during the Relocation lock state, SHALL be rejected by sending the *Relocation_Notify* set to the Reject value and the Failure Indication set to Locked state.

STEP 4

Upon receiving the *Relocation_Notify_Rsp* from the old ASN-GW with Accept/Rejection code set to accept value, the new ASN-GW caches the received NA_NONCE value, and sends RADIUS Access-Request or Diameter WDOR to the H-AAA. The Access-Request Message includes PA_VC, CMAC_KEY_COUNT and User-Name field set to MS-NAI.

If the received Accept/Rejection code is set to the reject value, the new ASN-GW revokes the optimized standalone authenticator relocation.

STEP 5

If HAAA supports the standalone authenticator Relocation, the H-AAA first checks that the value of the received OCR_COUNT is the same or larger than the internally maintained value of the OCR_COUNT.

The HAAA then verifies the PA_VC. If the validation is success, the H-AAA sends RADIUS Access-Accept or Diameter WDOA with the authorization parameters including the MSK and the MN-HA-PMIP4 or MAG-LMA-PMIP6 key with associated SPI value. Note, that the MAG-LMA-PMIP6 is associated with the address of the new Authenticator.

The H-AAA then sets the value of the OCR_COUNT = MAX (PA_NONCE, OCR_COUNT).

If H-AAA fails to verify the PA_VC, it sends RADIUS Access-Reject or Diameter WDEA with EAP Failure Indication.

STEP 6

The new ASN-GW sends the *Relocation_Complete_Req* message to the old ASN-GW (the present Authenticator) to complete the combined relocation. The message includes NA_VC generated by the new Authenticator generates as described in section 4.20.1.1.

STEP 7

Upon receiving the *Relocation_Complete_Req* message, the present Authenticator (the old ASN-GW in the diagram) verifies the NA_VC and sends back *Relocation_Complete_Rsp*. The message may include Accounting Context and PPAQ. The Anchor PC ID may be also included in the *Relocation_Complete_Rsp* message (Note 1).

STEP 8

Old Authenticator sends *Accounting Stop* message so that the H-AAA knows the present authenticator is no longer serving.

STEP 9

The new ASN-GW sends *Relocation_Complete_Ack*. Upon receiving *Relocation_Complete_Ack* from the new authenticator, the old authenticator terminates “relocation lock” state.

STEP 10

The new ASN-GW sends *Accounting Start* message so that the H-AAA knows the new Authenticator is now the Anchor Authenticator.

STEP 11 a

If the Anchor PC ID is present in the new authenticator the new Authenticator determines the MS/AMS is in Idle mode, and sends Context Rpt to the Anchor PC in order to update the Anchor Authenticator ID in case of idle MS.

STEP 11 b

If the Anchor PC ID is absent in the new authenticator, the new Authenticator determines the MS/AMS is in active mode, and sends Context Rpt to the current serving BS/ABS in order to update the Anchor Authenticator ID in case of active MS.

STEP 12 a

The Anchor PC responds the new ASN-GW by sending *Context Ack* in case of idle MS/AMS.

STEP 12 b

The serving BS/ABS responds the new ASN-GW by sending *Context Ack* in case of active MS/AMS.

Note 1: If applicable, the Anchor PC ID SHALL be included in either step 2 *Relocation_Notify_Rsp* or step 6 *Relocation_Complete_Rsp* and the new Authenticator SHALL store it for the MS/AMS.

Note 2: After authenticator relocation procedure happens, new authenticator SHALL inform the Anchor DP of the change of authenticator by sending *Context_Rpt* based on section 4.4.1.5.5.4 of WiMAX Forum® Network Architecture R1.5 specification.

4.21.2.2 Optimized Standalone Authenticator Relocation Error Scenarios

The Old ASN-GW proposes ‘Optimized Standalone Authenticator Relocation with OR Type set to 0x02.

Upon receiving the *Relocation Trigger* message, the New ASN-GW can behave as follows:

1) If the new ASN-GW doesn’t understand the *Relocation Trigger* message, it silently discards the message. Note that the old ASN-GW may re-try the procedure. It is implementation-specific how many times it retries.

2) If the new ASN-GW understands the *Relocation Trigger* message but it doesn't support the proposed OR Type but alternatively supports 'Optimized Combined Relocation' and the MS/AMS is in active mode , the New ASN-GW may proceed with the steps described in the section 4.20.2.2 'Optimized Combined Relocation'.

3) If the new ASN-GW understands the *Relocation Trigger* message, but if it decides to relocate the Authenticator with reauthentication of the MS/AMS, then it may proceed with the steps described in the unoptimized authenticator relocation procedure described in section 4.4.1.5.5.2.

4.21.3 Message and TLV definitions

Table 4-210 – Relocation_Trigger from "Old" Authenticator to "New" Authenticator

IE	Reference	M/O	Notes
MS Info	5.3.2.103	M	Contains MS-related context in the nested IEs.
> Optimized Relocation (OR) Type	5.3.2.232	CM	Indicates Optimized Relocation This TLV SHALL be included if the message is used for OR.
> Authenticator ID	5.3.2.19	O	Indicates the ID of the 'old' Authenticator GW.

4.22 Per SF Encryption Indicator Functional Overview

The per SF Airlink Encryption Indicator feature is an optional feature that allows the ASN to receive an airlink encryption policy, from the Home AAA or from the PDF/PCRF, and apply the policy to a specified service flow.

During the service flow establishment operation over the airlink, if the feature is supported by the ASN and if the SF Airlink Encryption Indicator is set to "off", the BS/ABS SHALL not encrypt the airlink corresponding with the service flow. If the SF Airlink Encryption Indicator is set to "on", the BS/ABS shall encrypt the corresponding service flow over the air.

Per IEEE 802.16-2009 [13], or IEEE 802.16m, once a service flow encryption policy is is applied; the BS/ABS and the MS/AMS SHALL consistently comply with it throughout the lifetime of the service flow, including during intra-ASN and inter-ASN handoffs.

4.22.1 Per SF Airlink Encryption On/Off Capability negotiation and Backward Compatibility Support

4.22.1.1 ASN Capability Negotiation for Per SF Airlink Encryption

NAP policy regarding the per SF airlink encryption on/off capability SHALL be consistent across the NAP.

An ASN-GW MAY be preprovisioned with the encryption policy or MAY negotiate the on/off encryption capability with peer BSs over R6.

An ASN GW SHALL transfer the SF airlink encryption capability during the MS/AMS' anchor functions relocation over R4 (for Authenticator/ Anchor SFA/ A-PCEF relocation).

4.22.1.2 ASN-AAA Capability Negotiation for Pre-Provisioned Service Flow

During the MS/AMS initial network entry, the NAS and the AAA exchanges the WiMAX Packet-Flow-Operation-Policy capability which includes the service flow airlink encryption on/off capability.

If the per SF airlink encryption on/off capability is set to "off" or the Packet-Flow-Operation-Policy is not present during the WiMAX Capability exchange in the Access-Request message, it implies that the ASN does not support per SF airlink encryption on/off capability. In this case, the AAA shall NOT include any SF-Operation-Policy in the Flow Spec in the Access-Accept message.

In the event if AAA includes SF-Operation-Policy in the Flow Spec while the ASN has previously indicated not supporting the per SF airlink encryption on/off capability, the ASN may ignore such policy setting.

The “absence” of the Packet-Flow-Operation-Policy in the Access-Request message implies that the airlink encryption is a local implementation policy at the ASN.

Otherwise, if the per SF airlink encryption on/off capability is set to “on”, this implies that the ASN supports the capability. In such scenario, the AAA may include the SF-Operation-Policy in the Flow Spec in the Access-Accept message to indicate the per SF airlink encryption on/off policy.

If the ASN has indicated the support for the per SF airlink encryption on/off capability, but the AAA does not provide the SF-Operation-Policy in the Flow Spec in the Access-Accept message, the airlink encryption for a given service flow will then follow local implementation policy of the ASN.

When the ASN receives the per SF airlink encryption on/off policy from the AAA, the MS/AMS’ Authenticator/Anchor SFA anchor ASN-GW SHALL pass on the policy setting in the SF-Operation-Policy over R6 or R6/R4 to the serving BS/ABS.

4.22.1.3 PCC Capability Negotitiation between A-PCEF and PDF/PCRF

Refer to WiMAX PCC Specification [3], section 7.5.

4.22.1.4 Handover and Idle Mode Exit Impacts

After the handover and the IM exit procedures, the airlink handling between the MS/AMS and the BS/ABS SHALL continue to comply with the IEEE 802.16-2009 specification [13] section 6.3.3.6 or the IEEE 802.16m section 16.2.4.6 “Encryption of MAC PDUs”.

4.23 [place holder]

4.24 ASN LOCALIZED ROUTING

The ASN Localized Routing (ALR) feature involves in creating a direct data-path between two peer-to-peer communicating MSs whose data paths are anchored at the same ASN-GW. The Anchor ASN-GW creates the direct path between the peers. An ALR-enabled ASN-GW can allow IP traffic to directly flow between the MSs without traversing the CSN(s). Enabling ALR on an end-to-end flow requires the involvement of the ASN and CSN(s) to support the ALR feature, the CSN(s) to authorize ALR on service flows composing the end-to-end flow, and the ASN to detect the end-to-end service flow and establishing a local datapath.

Local Routing Policy is received from the Home AAA or from the PDF/PCRF, and is applied to a specified service flow. However, it should be noted that for roaming cases the Local Routing Policy received from the Home AAA or PDF/PCRF may be altered by the VCSN. The Local Routing Policy, which is service-flow-based rule(s) for performing ASN Local Routing, is stored in the HAAA/SPR as the user’s subscription ALR attribute. Pre-provisioning and updates of a per flow Local Routing Policy in the PDF/PCRF/Home AAA is out of scope for this specification.

The R3/R5 PMIP tunnel, or the Simple IP transport, is always established between the ASN and CSN(s) irrespective of whether and when ALR is enabled. The PMIP tunnel or Simple IP transport is unconditionally setup at the time of Initial Network Entry and is not torn down based on ALR actions. These tunnel/transports are not used for ALR-enabled flows, but that does not allow tearing them down because tearing them down implies the MS is exiting the network. Tearing down the tunnel/transport when ALR is enabled and re-establishing the tunnel/transport when ALR is terminated, is left for a future study.

Note: For the CMIP cases, since the E2E MIP tunnel is eststablished between the MS and HA/LMA, ALR is not supported for CMIP in this release.

To summarize, ASN Local Routing is a function that optimizes media data (bearer) traffic delivery between two end points by locally routing the packets within the WiMAX access network. ASN Local Routing Control Point is the entity where Local Routing Policy is available and which is responsible for controlling Local Routing behavior. The ASN Local Routing Enforcement Point is an ASN node (ASN-GW), which has Local Routing capability, and is responsible for enforcing the local routing of media data traffic. The ASN Local Routing Policy (e.g. PCC) is a set of rules that controls the Local Routing behavior. The Local Routing rules reside with the NSP and are forwarded to the NAP for enforcement.

4.24.1 CAPABILITY NEGOTIATION AND POLICY AUTHORIZATION

During the MS initial network entry, the NAS, the VAAA, and HAAA exchange the ALR capability.

ASN and CSN(s) must indicate their ALR support by using Local-Routing-Support TLV in WiMAX-Capability VSA during the INE of the MS. ALR will be used only if it's successfully negotiated as a supported feature.

If HCSN indicates it supports ALR, HCSN must also include a Local-Routing-Policy VSA in the RADIUS Access-Accept packet or WDEA packet with Result-Code AVP indicating success during the MS' INE procedure. HCSN must set the Local Routing Policy value of this AVP to 0 (No ALR) if it wants to disallow ALR for a given service flow of MS. If the value is set to 1 (Pre-Authorized ALR), that means the ASN can perform ALR for the given service flow as soon as it detects an end-to-end flow. Local Routing Policy value set to 2 (Dynamic-Authorized ALR) indicates that the HCSN will dynamically authorize the ASN to perform ALR. An ASN may dynamically request ALR by a separate request procedure to CSN, if it detects that ALR can be initiated.

For roaming cases, ALR support must be indicated by both the HCSN and VCSN. If the VCSN receives a RADIUS Access-Accept packet or WDEA packet with Result-Code AVP indicating success during the MS' INE procedure, then the VCSN shall reset the Authorization value of this AVP based on its policy and the Authorization value set by the HCSN in the received packet. After resetting the Authorization value the VCSN shall forward the packet to the ASN. The VCSN may reset the Authorization value to be more restrictive than the value in the received packet, but shall not reset the Authorization value to be less restrictive. The allowed Authorization value settings to be used by the VCSN are summarized in Table 4-211. Other permutations are not allowed. Note that if the VCSN does not support ALR, the VCSN shall always set the Authorization value to 0.

Table 4-211 – VCSN population of ALR Authorization value

Authorization value in packet received from HCSN	Values to which the VCSN may set the Authorization value
0 (No ALR)	0
1 (Pre-Authorized ALR)	0, 1, 2
2 (Dynamic-Authorized ALR)	0, 2

When the ASN receives Local Routing Policy from the AAA or VCSN, the MS' Authenticator/Anchor SFA shall decide whether ALR is allowed for the given service flow per the received policy and the local policy. If ALR is allowed, the MS' Authenticator/Anchor SFA shall deliver the Local Routing Policy over R4 to the serving SFA. If the ASN does not receive Local Routing Policy from the AAA, the given service flow shall follow the general service flow procedures.

Local Routing Policy delivery between A-PCEF and PDF/PCRF is specified in WiMAX PCC Specification [3], section 6.5.2.

4.24.1.1 ALR DURING HANDOFF

The ALR capability negotiated between the HCSN, VCSN and the ASN-GW is optional. Once negotiated and established, the capability SHOULD continue to be provided for the entire session. However, during handover, if the target gateway does not support ALR, the session SHALL continue without ALR. (i.e., since ALR is optional, the target gateway will accept the HO attempt regardless of ALR being supported or not).

4.24.2 ALR DETECTION BY ASN-GW

For each service flow whose Local Routing Policy=1 (Pre-Authorized ALR) or 2 (Dynamic-Authorized ALR), the ASN-GW shall invoke the detection procedure.

According to the detection procedure, when an uplink IP packet is received from MS1 over a service flow SF1 whose Local Routing Policy=1 (Pre-Authorized ALR) or 2 (Dynamic-Authorized ALR), the ASN-GW checks the source and destination IP addresses (IP1, IP2) of the received packet. The ASN GW checks the destination MS's location per the destination IP address. If both of the addresses are globally routable and both MSs are anchored on the ASN GW, then the ASN-GW checks if it also has a downlink service flow using the destination IP address and having its Local Routing Policy set to 1 (Pre-Authorized ALR) or 2 (Dynamic-Authorized ALR).

If there is a reverse traffic sent from MS2 to MS1, that traffic will also be subjected to the same detection procedure. ALR will be enabled in that direction depending on the authorization policy of the associated service flows.

4.24.3 USE OF ALR FOR COMMUNICATIONS SUBJECT TO LAES

If the WiMAX-SP providing ASN functionality detects a service flow for which ALR may be enabled as defined in section 4.24.2, and that service flow is subject to interception and reporting under Lawfully Authorized Electronic Surveillance (LAES), the ASN shall only enable ALR if doing so does not disrupt the ability to perform the intercept as required by national law or regulation. At INE the WiMAX-SP shall only authorize use of ALR for a session (i.e., set Local Routing Policy to 1 (Pre-Authorized ALR) or 2 (Dynamic-Authorized ALR)) if doing so would not disrupt the ability to perform an intercept as required by national law or regulation. A WiMAX-SP shall only allow an ASN Gateway to enable ALR for a service flow (i.e., send a RADIUS CoA message with ALR Command Action = Start or send a RADIUS Access_Accept message with ALR Command Action = Accepted in response to a RADIUS Access_Request message with ALR Command Action = Start) if doing so would not disrupt the ability to perform an intercept as required by national law or regulation.

If the WiMAX-SP receives an LAES order for communications for which ALR has already been enabled, the WiMAX-SP shall expeditiously disable ALR for each service flow subject to that LAES order unless the continued use of ALR will not disrupt the ability to perform the intercept as required by national law or regulation.

Disruption of the ability to perform the intercept is defined as causing some or all of the required communication content or communication identifying information associated with the service flow, or with the MS or WFAP that is the subject of the LAES order, not to be intercepted and reported when it would have been intercepted and reported if ALR were not enabled. Note that [121] identifies the specifications containing the LAES requirements that apply to different types of communications in different regions.

Note: it is recognized that not enabling or disabling ALR for communications subject to an LAES order as described above may result in changes in performance characteristics such as latency that may be perceptible to the subject of the LAES order.

4.24.4 ALR SUPPORTED CASES

There are two ASN-CSN pairing cases, where ALR is supported. In the first case, the two communicating MSs are using the same ASN-GW, HCSN, and VCSN (if they are roaming). In the second case, the two communicating MSs are using the same ASN-GW, but different HCSNs. They may or may not be using the same VCSN, if they are roaming.

4.24.4.1 COMMON ASN-GW, HCSN, AND VCSN

In this case, data path for the two service flows associated with the end-to-end flow are anchored on the same ASN-GW and the same HCSN. If the MSs are roaming, they are also using the same VCSN.

Consider MS1 with IP address IP1 using uplink service flow SF1, and MS2 with IP address IP2 using downlink service flow SF2. Both SF1 and SF2 are anchored on the same ASN-GW. MS1 is sending IP packets to MS2.

If both SFs have Local Routing Policy=1 (Pre-Authorized ALR), then the ASN-GW detection will identify the end-to-end flow and enable ALR.

If the ASN-GW received Local Routing Policy=2 (Dynamic_Authorized ALR) for one of the service flows and Local Routing Policy=1 (Pre_Authorized ALR) for the other, or Local Routing Policy=2 (Dynamic_Authorized ALR) for both, then it must not apply ALR until it obtains the Local Routing Policy from the HCSN by a sending a ALR request for the Dynamically Authorized service flow. ALR will be enabled only after the ASN GW receives authorization for all the dynamic authorized service flows. In accordance with the NAP policies, ASN-GW should send a RADIUS Access-Request with ALR Command, and shall not enable ALR unless it receives an approval from the HCSN. If the HCSN rejects the ALR request, then the ASN-GW should not send another ALR request for the same pair of service flows. Nevertheless, HCSN reserves the right to instantiate ALR on the very same pair of service flows at a later time at its will (by sending a CoA).

4.24.4.1.1 SCENARIO: ASN-INITIATED ALR START, ACCEPTED BY HCSN

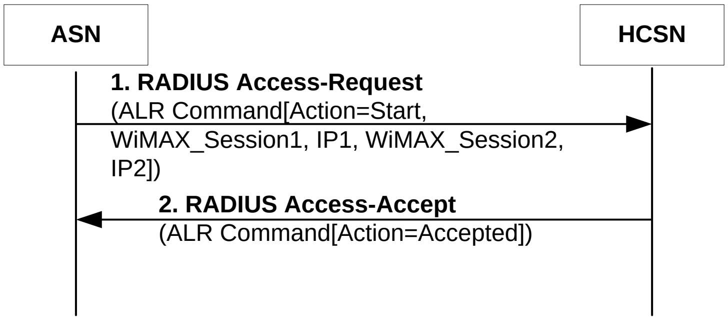

ASN
HCSN
1. RADIUS Access-Request
(ALR Command[Action=Start,
WiMAX_Session1, IP1, WiMAX_Session2,
IP2])
2. RADIUS Access-Accept
(ALR Command[Action=Accepted])

Figure 4-222 – ALR Request sent by ASN-GW to initiate ALR (non-roaming)

STEP 1

Upon detecting an end-to-end flow to which ALR can applied, the ASN-GW sends a RADIUS Access-Request packet to the HCSN containing ALR_Command AVP. The payload of the AVP indicates Action=Start, and provide the WiMAX session identifier and IP address for the two MSs of the end-to-end flow.

STEP 2

HCSN responds back with a RADIUS Access-Accept packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

4.24.4.1.2 SCENARIO: ASN-INITIATED ALR START, REJECTED BY VCSN

When the MS is roaming, the ALR authorization request is sent from the ASN to the HCSN via the VCSN. In that case, the ALR authorization request may also be rejected by the VCSN. The VCSN has two possible roles in processing the ALR authorization: Directly (i.e., without altering) forwarding the request/response to the HCSN, and rejecting the request when received from the ASN. The VCSN may decide to reject the ALR request for multiple reason such as LI requirement (Section 4.24.3). On the other hand, the VCSN has no authority to accept the ALR authorization request without authorization from the HCSN.

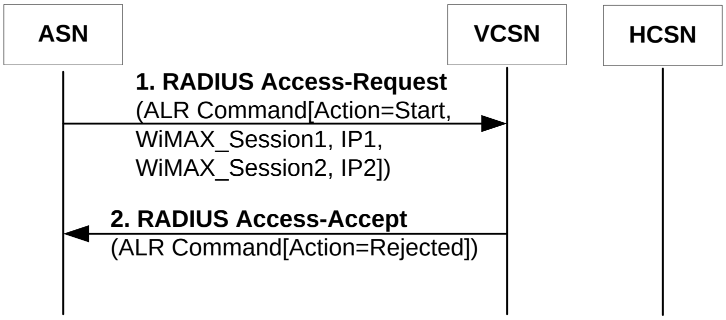


Figure 4-223 – ALR command sent by ASN-GW and rejected by VCSN (roaming)

STEP 1

Upon detecting the end-to-end flow that can be applied ALR, the ASN-GW sends a RADIUS Access-Request packet to the VCSN containing ALR_Command AVP. The payload of the AVP indicates Action=Start, and provides the WiMAX session identifier and IP address for the two end-points of the end-to-end flow.

STEP 2

Upon deciding to reject the ALR request, the VCSN responds back with a RADIUS Access-Accept packet containing ALR_Command AVP. The Action field of the AVP carries the value 3 (Rejected) in order to indicate a rejection of the ALR request.

ALR is terminated by the ASN-GW when one or both anchor DPFs relocate during handoff, or when the ASN-GW receives ALR_Command with Action= Stop for the end-to-end flow.

4.24.4.1.3 SCENARIO: HCSN-INITIATED ALR TERMINATION.

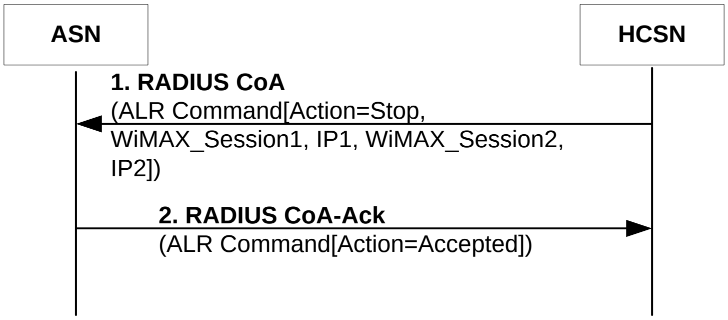

ASN
HCSN
1. RADIUS CoA
(ALR Command[Action=Stop,
WiMAX_Session1, IP1, WiMAX_Session2,
IP2])
2. RADIUS CoA-Ack
(ALR Command[Action=Accepted])

Figure 4-224 – ALR command sent by HCSN to terminate ALR (non-roaming)

STEP 1

When the HCSN decides to terminate the ALR for any reason, theHCSN sends a RADIUS CoA packet to the ASN-GW containing ALR_Command AVP. The payload of the AVP indicates Action=Stop, and provide the WiMAX session identifier and optionally the IP addresses for the two end-points of the end-to-end flow. IP addresses are omitted when the HCSN intends to terminate all of the ALR sessions associated with the WiMAX session.

STEP 2

The ASN-GW responds back with a RADIUS CoA-Ack packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

4.24.4.1.4 SCENARIO: VCSN-INITIATED ALR TERMINATION.

The same call flow is followed for HCSN-initiated ALR termination when the MS is roaming, except that the signaling goes via the VCSN in between the ASN and the HCSN. The VCSN shall forward the ALR_Command without any modifications. If the VCSN decides to terminate an on-going ALR session, it can do so as well. The VCSN may decide to terminate the ALR session for the LI reasons (Section 4.24.3). There may be other reasons outside the scope of this specification. Details of how the VCSN decides to terminate an ALR session are outside the scope of this specification.

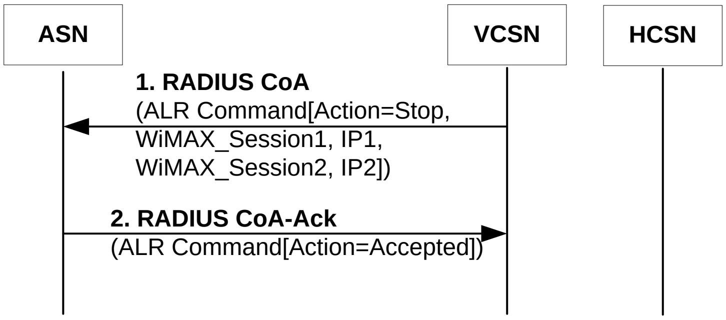


Figure 4-225 – ALR command sent by VCSN to terminate ALR (roaming)

STEP 1

When the VCSN decides to terminate the ALR for any reason, the VCSN sends a RADIUS CoA packet to the ASN-GW containing ALR_Command AVP. The payload of the AVP indicates Action=Stop, and provides the WiMAX session identifier and optionally the IP addresses for the two end-points of the end-to-end flow. IP addresses are omitted when the VCSN intends to terminate all of the ALR sessions associated with the WiMAX session.

STEP 2

The ASN-GW responds back with a RADIUS CoA-Ack packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

4.24.4.1.5 SCENARIO: HCSN-INITIATED ALR RE-START

The HCSN may decide to initiate ALR after it stopped an earlier instance, or after it rejected an earlier request by the ASN-GW. In order to do that, the HCSN shall send ALR command with Action=Start. What triggers the restoration/initiation of ALR is out of scope.

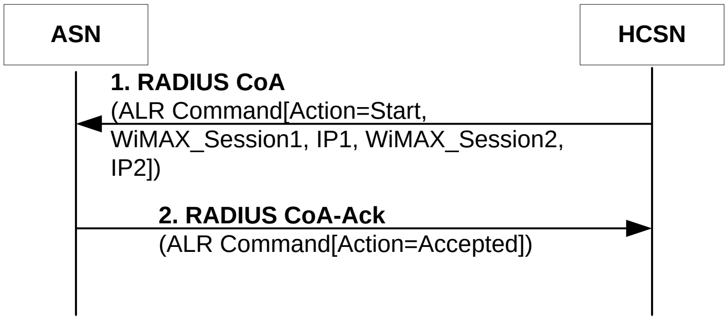

ASN
HCSN
1. RADIUS CoA
(ALR Command[Action=Start,
WiMAX_Session1, IP1, WiMAX_Session2,
IP2])
2. RADIUS CoA-Ack
(ALR Command[Action=Accepted])

Figure 4-226 – ALR command sent by HCSN to start ALR (non-roaming)

STEP 1

When the HCSN decides to start the ALR, the HCSN sends a RADIUS CoA packet to the ASN-GW containing ALR_Command AVP. The payload of the AVP indicates Action=Start, and provides the WiMAX session identifier and IP address for the two end-points of the end-to-end flow.

STEP 2

The ASN-GW responds back with a RADIUS CoA-Ack packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

4.24.4.1.6 SCENARIO: VCSN-INITIATED ALR RE-START.

The VCSN may decide to initiate ALR after it stopped an earlier instance, or after it rejected an earlier request by the ASN-GW. See Section 4.24.5 for the specific conditions under which a VCSN is allowed to initiate ALR. The VCSN shall send ALR command with Action=Start in order to initiate ALR. What triggers the restoration/initiation of ALR is out of scope.

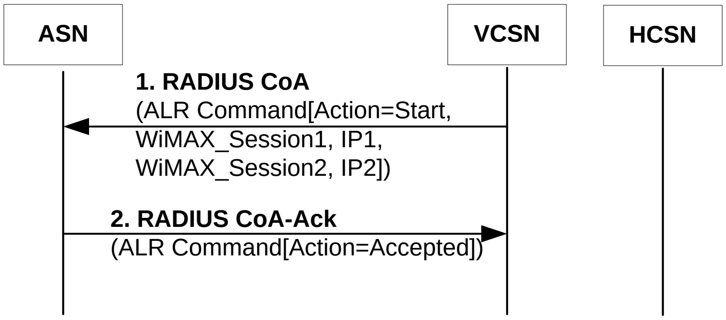


Figure 4-227 – ALR command sent by VCSN to initiate ALR (roaming)

STEP 1

When the VCSN decides to start the ALR, the VCSN sends a RADIUS CoA packet to the ASN-GW containing ALR_Command AVP. The payload of the AVP indicates Action=Start, and provides the WiMAX session identifier and the IP addresses for the two end-points of the end-to-end flow.

STEP 2

The ASN-GW responds back with a RADIUS CoA-Ack packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

4.24.4.2 COMMON ASN-GW, COMMON OR SEPARATE VCSNS, SEPARATE HCSNS

In this case, data path for the two service flows associated with the end-to-end flow are anchored on the same ASN-GW but separate HCSNs. If the MSs are roaming, they may or may not be using the same VCSN.

Consider MS1 with IP address IP1 using uplink service flow SF1, and MS2 with IP address IP2 using downlink service flow SF2. Both SF1 and SF2 are anchored on the same ASN-GW. But MS1's data path is anchored in CSN1, whereas MS2's data path is anchored in CSN2. MS1 is sending IP packets to MS2.

If one or both of the SFs have Local Routing Policy=0 (No ALR), then ASN-GW will not perform ALR.

If both SFs have Local Routing Policy=1 (Pre-Authorized ALR), then the ASN-GW detection will identify the end-to-end flow and the ASN-GW can enable ALR.

If the ASN-GW received Local Routing Policy=2 (Dynamic_Authorized ALR) for one of the service flows and Local Routing Policy=1 (Pre_Authorized ALR) for the other, or Local Routing Policy=2 (Dynamic_Authorized ALR) for both, then it must not apply ALR autonomously, instead when local routing conditions are met (refer to Section 4.24.2: Detection by ASN-GW), it must start ALR authorization procedure with CSN for the dynamically authorized service flow. Instead, the ASN-GW should request dynamic authorization from the CSN(s) that has/have indicated Dynamic_Authorized ALR. The ASN-GW should apply ALR if the associated service flows are either marked as Pre-Authorized ALR or the ASN-GW has dynamically obtained the necessary authorization. Call flow in Figure 4-228 depicts this case.

4.24.4.2.1 SCENARIO: ASN-INITIATED ALR START, ACCEPTED BY HCSNS.

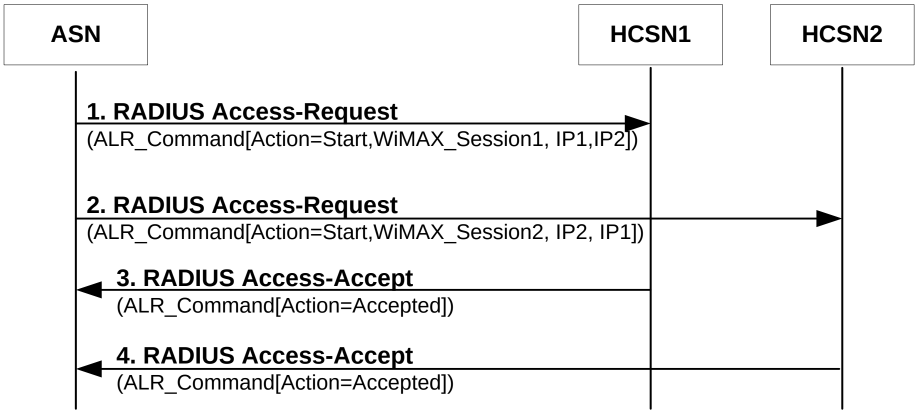

ASN
HCSN1
HCSN2
1. RADIUS Access-Request
(ALR_Command[Action=Start,WiMAX_Session1, IP1,IP2])
2. RADIUS Access-Request
(ALR_Command[Action=Start,WiMAX_Session2, IP2, IP1])
3. RADIUS Access-Accept
(ALR_Command[Action=Accepted])
4. RADIUS Access-Accept
(ALR_Command[Action=Accepted])

Figure 4-228 – ALR command sent by ASN-GW to initiate ALR (non-roaming)

STEP 1

Upon detecting that there is an end-to-end flow between two MSs that are from two separate HCSNs, and none of the service flows have Local Routing Policy=0 (No ALR), the ASN-GW sends a RADIUS *Access-Request* message to HCSN1 for obtaining dynamic Local Routing Policy if the HCSN1 had marked the SF with Local Routing Policy=2 (Dynamic-Authorized ALR). This step is only performed if Local Routing Policy=2 (Dynamic-Authorized ALR).

The payload of the RADIUS VSA indicates Action=Start, and provides the WiMAX session identifier associated with the service flow managed by the HCSN1 and the IP addresses for the two end-points of the end-to-end flow.

STEP 2

Upon detecting that there is an end-to-end flow between two MSs that are from two separate HCSNs, and none of the service flows are marked with Local Routing Policy=0 (No ALR), the ASN-GW sends a RADIUS Access-Request message to HCSN2 for obtaining dynamic authorization if HCSN2 had marked the SF with Local Routing Policy=2 (Dynamic-Authorized ALR). This step is only performed if Local Routing Policy=2 (Dynamic-Authorized ALR).

The payload of the RADIUS VSA indicates Action=Start, and provides the WiMAX session identifier associated with the service flow managed by the HCSN2 and the IP addresses for the two end-points of the end-to-end flow.

STEP 3

If HCSN1 has received an ALR dynamic authorization request, it processes the request and responds.

STEP 4

If HCSN2 has received an ALR dynamic authorization request, it processes the request and responds.

If the ASN-GW received ALR Command with Action= Accepted from the HCSN(s) that it has sent a request(s), it enables ALR on the end-to-end flow. If one or both of the responses are not received, or anyone is received with a result code Not Accepted, then the ASN-GW can’t enable ALR.

The same call flow is followed when the MS is roaming, except that the signaling goes via the VCSN(s) in between the ASN and the HCSN(s). The VCSN(s) has the option to forward the ALR Command without any modifications or reject the request.

ALR is terminated by the ASN-GW when one or both anchor DPFs relocate or when the ASN-GW receives ALR_Command with Action=Terminate for one of the flows.

4.24.4.2.2 SCENARIO: ASN-INITIATED ALR START, REJECTED BY ONE OF THE VCSNS.

When the MS is roaming, the ALR authorization request is sent from the ASN to the HCSN1 via the VCSN1. In that case, the ALR authorization request may also be rejected by the VCSN1. The VCSN1 has two possible roles in processing the ALR authorization: Directly (i.e., without altering) forwarding/accepting the request/response to/from the HCSN1, and rejecting the request when received from the ASN. The VCSN1 may decide to reject the ALR request for many reasons such as LI requirements (Section 4.24.3). On the other hand, the VCSN1 has no authority to accept the ALR authorization request without authorization from HCSN1.

In this call flow only the ASN-VCSN1-HCSN1 part is shown. Assume ASN-VCSN2-HCSN2 signaling is executed as outlined in the previous scenario.

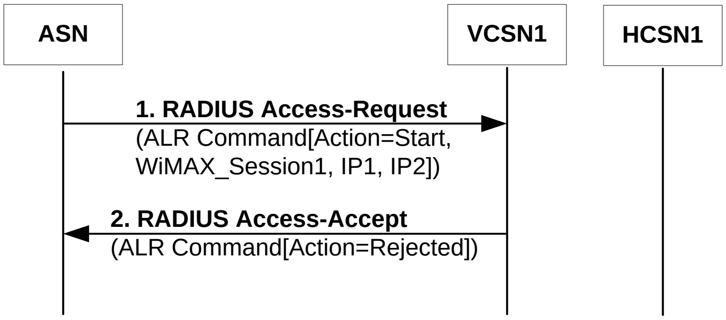

ASN
VCSN1
HCSN1
1. RADIUS Access-Request
(ALR Command[Action=Start,
WiMAX_Session1, IP1, IP2])
2. RADIUS Access-Accept
(ALR Command[Action=Rejected])

Figure 4-229 – ALR command sent by ASN-GW and rejected by VCSN (roaming)

STEP 1

Upon detecting the end-to-end flow that can be applied ALR, the ASN-GW sends a RADIUS Access-Request packet to the HCSN via the VCSN containing ALR_Command AVP. The payload of the AVP indicates Action=Start, and provides the WiMAX session identifier associated with the HCSN1 and IP address for the two end-points of the end-to-end flow.

STEP 2

Upon deciding to reject the ALR request, the VCSN responds back with a RADIUS Access-Accept packet containing ALR_Command AVP. The Action field of the AVP carries the value 3 (Rejected) in order to indicate rejection of the ALR request.

Even though the ASN may receive a RADIUS Access-Accept with the Action field carrying value 2 (Accepted) from the other HCSN (i.e. HCSN2), the ASN can’t initiate the ALR as it did not obtain authorization from both HCSNs.

4.24.4.2.3 SCENARIO:HCSN-INITIATED ALR TERMINATION.

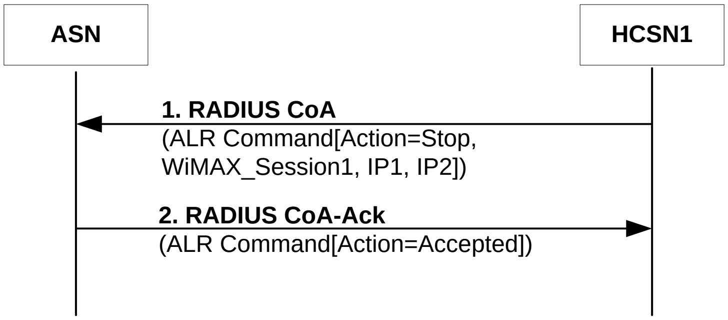

ASN
HCSN1
1. RADIUS CoA
(ALR Command[Action=Stop,
WiMAX_Session1, IP1, IP2])
2. RADIUS CoA-Ack
(ALR Command[Action=Accepted])

Figure 4-230 – ALR command sent by one of the HCSNs (HCSN1) to terminate ALR (non-roaming)

STEP 1

When one of the HCSNs decides to terminate the ALR for any reason, that HCSN sends a RADIUS CoA packet to the ASN-GW containing ALR_Command AVP. The payload of the AVP indicates Action=Stop, and provides the WiMAX session identifier associated with the flow managed by that HCSN, and optionally the IP addresses for the two end-points of the end-to-end flow. IP addresses are omitted when the HCSN intends to terminate all of the ALR sessions associated with the WiMAX session.

STEP 2

The ASN-GW responds back with a RADIUS CoA-Ack packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

The same call flow is followed when the MS is roaming, except that the signaling goes via the VCSN in between the ASN and the HCSN.

4.24.4.2.4 SCENARIO: VCSN-INITIATED ALR TERMINATION.

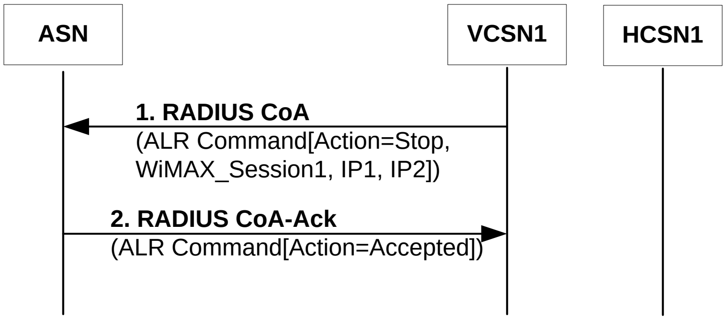

ASN
VCSN1
HCSN1
1. RADIUS CoA
(ALR Command[Action=Stop,
WiMAX_Session1, IP1, IP2])
2. RADIUS CoA-Ack
(ALR Command[Action=Accepted])

Figure 4-231 – ALR command sent by VCSN to terminate ALR (roaming)

STEP 1

When the VCSN decides to terminate the ALR for any reason, the VCSN sends a RADIUS CoA packet to the ASN-GW containing ALR_Command AVP. The payload of the AVP indicates Action=Stop, and provides the WiMAX session identifier and optionally the IP addresses for the two end-points of the end-to-end flow. IP addresses are omitted when the VCSN intends to terminate all of the ALR sessions associated with the WiMAX session.

STEP 2

The ASN-GW responds back with a RADIUS CoA-Ack packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

4.24.4.2.5 SCENARIO:HCSN-INITIATED ALR RE-START

The same HCSN may decide to initiate ALR after it stopped an earlier instance, or after it rejected an earlier request by the ASN-GW. In order to do that, the HCSN shall send ALR command with Action=Start. ALR is (re-)initiated only if it is not stopped or rejected by the other HCSN at the time.

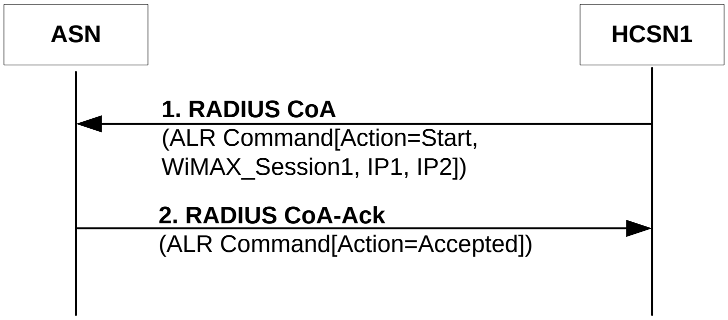

ASN
HCSN1
1. RADIUS CoA
(ALR Command[Action=Start,
WiMAX_Session1, IP1, IP2])
2. RADIUS CoA-Ack
(ALR Command[Action=Accepted])

Figure 4-232 – ALR command sent by one of the HCSNs to start ALR (non-roaming)

STEP 1

When one of the HCSNs decides to start the ALR, the HCSN sends a RADIUS CoA packet to the ASN-GW containing ALR_Command AVP. The payload of the AVP indicates Action=Start, and provides the WiMAX session identifier associated with the flow managed by the HCSN, and IP address for the two end-points of the end-to-end flow.

STEP 2

The ASN-GW responds back with a RADIUS CoA-Ack packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

4.24.4.2.6 SCENARIO:VCSN-INITIATED ALR RE-START.

One of the VCSNs may decide to initiate ALR after it stopped an earlier instance, or after it rejected an earlier request by the ASN-GW. See Section 4.24.5 for the specific conditions under which a VCSN is allowed to initiate ALR. The VCSN shall send ALR command with Action=Start in order to initiate ALR. What triggers the restoration/initiation of ALR is out of scope.

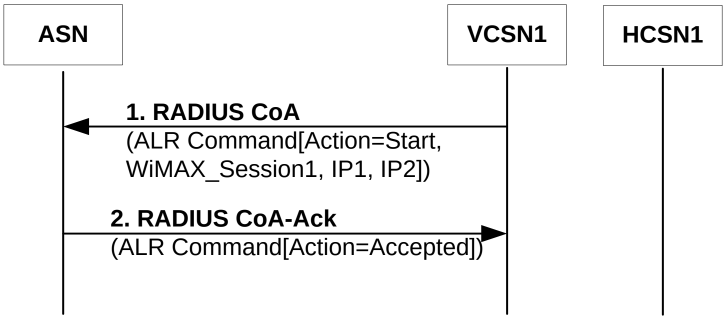

ASN
VCSN1
HCSN1
1. RADIUS CoA
(ALR Command[Action=Start,
WiMAX_Session1, IP1, IP2])
2. RADIUS CoA-Ack
(ALR Command[Action=Accepted])

Figure 4-233 – ALR command sent by VCSN to initiate ALR (roaming)

STEP 1

When the VCSN decides to start the ALR, the VCSN sends a RADIUS CoA packet to the ASN-GW containing ALR_Command AVP. The payload of the AVP indicates Action=Start, and provides the WiMAX session identifier associated with the flow managed by the VCSN, and the IP addresses for the two end-points of the end-to-end flow.

STEP 2

The ASN-GW responds back with a RADIUS CoA-Ack packet containing ALR_Command AVP. The Action field of the AVP indicates whether the command was accepted or not.

4.24.5 REQUIREMENTS FOR CONTROL OF ALR THROUGH ALR COMMAND

The ASN and CSN(s) control the enabling and disabling of ALR for a given service flow through the use of the ALR Command contained in the RADIUS *Access_Request* / *Access_Accept*, or *CoA* / *CoA_Ack* messages.

4.24.5.1 ASN CONTROL OF ALR

When the ASN, using the detection process defined in 4.24.2, identifies a service flow with Authorization value = 2 (Dynamic-Authorized ALR) for which it wishes to enable ALR, the ASN SHALL send a RADIUS *Access_Request* message with ALR Command Action = Start to the CSN. The ASN SHALL only enable ALR if it subsequently receives a RADIUS *Access_Accept* message with ALR Command Action = Accepted. If the two service flows associated with an end to end flow are anchored to different CSNs, then a RADIUS *Access_Request*/*Access_Accept* message SHALL be sent to/received from each CSN for which the corresponding service flow has an Authorization value = 2 (Dynamic-Authorized ALR). If the ASN receives a RADIUS *Access_Accept* message with ALR Command Action = Rejected, then the ASN SHALL not send any additional ALR related RADIUS *Access_Request* messages for the service flow until such time as it receives a RADIUS *CoA* message with ALR Command Action = Start.

If the ASN receives a RADIUS *CoA* message with ALR Command Action = Stop, the ASN SHALL terminate ALR for the service flow indicated in the RADIUS *CoA* message and SHALL send a RADIUS *CoA_Ack* message with ALR Command Action = Accepted. Thereafter, the ASN SHALL not enable ALR for any service flows associated with the session(s) indicated in the RADIUS *CoA* message until it receives a RADIUS *CoA* message with ALR Command Action = Start. If no IP addresses are included in the RADIUS *CoA* message, then the ASN SHALL terminate ALR for all service flows associated with the indicated session(s).

If the ASN receives a RADIUS *CoA* message with ALR Command Action = Start, the ASN MAY enable ALR for detected service flows associated with the session indicated in the RADIUS *CoA* message and SHALL send a RADIUS *CoA_Ack* message with ALR Command Action = Accepted. Whether ALR is enabled for a given service flow associated with the session indicated in the RADIUS *CoA* message, is thereafter governed by the Authorization value ALR Command received from the CSN during INE.

4.24.5.2 HCSN CONTROL OF ALR

When the HCSN receives a RADIUS *Access_Request* message with ALR Command Action = Start, the HCSN SHALL respond with a RADIUS *Access_Accept* message with ALR Command Action = Accepted if its policy is to allow ALR for the service flow(s) indicated in the received RADIUS *Access_Request* . Otherwise, the HCSN SHALL respond with a RADIUS *Access_Accept* message with ALR Command Action = Rejected.

If the HCSN desires to allow ALR for a given service flow at a given ASN Gateway after it has rejected a RADIUS *Access_Request* message with ALR Command Action = Start for that service flow from that ASN Gateway, or has previously sent a RADIUS *CoA* message with ALR Command Action = Stop, the HCSN SHALL send a RADIUS *CoA* message with ALR Command Action = Start.

If the HCSN desires to stop (disable) ALR for a given service flow at a given ASN Gateway, the HCSN SHALL send a RADIUS *CoA* message with ALR Command Action = Stop. If the HCSN desires to stop (disable) ALR for all service flows associated with a given session at the ASN Gateway, the HCSN SHALL send a RADIUS *CoA* message with ALR Command Action = Stop and none of the IP Address parameters included.

4.24.5.3 VCSN CONTROL OF ALR

When the VCSN receives a RADIUS *Access_Request* message with ALR Command Action = Start, the VCSN MAY forward it to the HCSN if its policy is to allow ALR for the indicated service flow. If the VCSN is not authorized by the HCSN to enable ALR, the VCSN SHALL send a RADIUS *Access_Accept* message with ALR Command Action = Rejected to the ASN.

If after requesting authorization, the VCSN receives a RADIUS *Access_Accept* message from the HCSN, the VCSN SHALL forward it to the ASN.

When the VCSN receives a RADIUS *CoA* message with ALR Command Action = Stop from the HCSN, the VCSN SHALL forward it to the ASN.

When the VCSN receives a RADIUS *CoA* message with ALR Command Action = Start from the HCSN, the VCSN MAY forward the message to the ASN if its policy is to allow ALR for the indicated service flow. If the VCSN does not forward the RADIUS *CoA* message, the VCSN SHALL send a RADIUS *CoA_Ack* message with ALR Command Action = Rejected to the ASN.

If the VCSN desires to allow ALR for a given service flow at a given ASN Gateway after it has rejected a RADIUS *Access_Request* message with ALR Command Action = Start for that service flow from that ASN Gateway, or has previously sent a RADIUS *CoA* message with ALR Command Action = Stop, the VCSN SHALL send a RADIUS *CoA* message with ALR Command Action = Start. The VCSN SHALL only send a RADIUS *CoA* message with ALR Command Action = Start when one of the following conditions exists:

- The RADIUS *CoA* message is being sent (forwarded) based on a RADIUS *CoA* message with ALR Command Action = Start received from the HCSN;
- The VCSN previously received a RADIUS *CoA* message with ALR Command Action = Start from the HCSN but did not forward it to the ASN Gateway and the VCSN has not subsequently received a RADIUS *CoA* message with ALR Command Action = Stop from the HCSN.
- The Authorization value received from the HCSN at Initial Network Entry for the service flow is 1(Pre-Authorized ALR) and no subsequent ALR Command Action = Stop was received from the HCSN that was not itself followed by an ALR Command Action = Start.

If the VCSN desires to stop (disable) ALR for a given service flow at a given ASN Gateway, the VCSN SHALL send a RADIUS *CoA* message with ALR Command Action = Stop. If the VCSN desires to stop (disable) ALR for all service flows associated with a given session at the ASN Gateway, the VCSN SHALL send a RADIUS *CoA* message with ALR Command Action = Stop and none of the IP Address parameters included.

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	*RR_Req*	Table 4-34, Table 4-63, Table 4-64, Table 4-65, Table 4-66, Table 4-67
	2	010	*RR_Rsp*	Table 4-35, Table 4-68, Table 4-69,
	3	011	*RR_Ack*	Table 4-70
2 (HO Control)	1	001	*HO_Req*	Table 4-86, Table 4-108, Table 4-115, Table 4-118
	2	010	*HO_Rsp*	Table 4-89

Function Type	Msg Type	OP ID	Message	Message Layout
	3	011 for the 3-way Handshake and 010 in case of 2-way transaction	*HO_Ack*	Table 4-90
	4	001	*HO_Cnf*	Table 4-94, Table 4-95
	5	001	*HO_Complete*	Table 4-103
	6	001	*HO_Directive*	
	7	010	*HO_Directive_Rsp*	
3 (Data Path Control)	1	001	*Path_Dereg_Req*	Table 4-37, Table 4-79
	2	010	*Path_Dereg_Rsp*	Table 4-80
	3	011	*Path_Dereg_Ack*	This message does not contain any TLVs, so there is no message layout.
	4	001	*Path_Modification_Req*	Table 4-76
	5	010	*Path_Modification_Rsp*	Table 4-77
	6	011	*Path_Modification_Ack*	Table 4-78
	7	001	*Path_Prereg_Req*	Table 4-91
	8	010	*Path_Prereg_Rsp*	Table 4-92
	9	011	*Path_Prereg_Ack*	Table 4-93
	10	001	*Path_Reg_Req*	Table 4-98
	11	010	*Path_Reg_Rsp*	Table 4-99
	12	011	*Path_Reg_Ack*	Table 4-100, Table 4-177, Table 4-182
	13	100	*IM_Exit_State_Ind*	Table 4-180
	14	011	*IM_Exit_State_Ind_Ack*	Table 4-181
4 (Context Transfer)	1	001	*Context_Req*	Table 4-87, Table 4-161
	2	010 (for the report sent in response to *Context_Req* message) and 001(Report sent without *Context_Req* message and waiting for *Context_Ack* message)	*Context_Rpt*	Table 4-22, Table 4-33, Table 4-88, Table 4-162, Table 4-121
	3	010	*Context_Ack*	Table 4-23, Table 4-122
	4	001	*CMAC_Key_Count_Update*	Table 4-101

Function Type	Msg Type	OP ID	Message	Message Layout
	5	010	*CMAC_Key_Count_Update_Ack*	Table 4-102
	6	-	*VOID*	
	7	-	*VOID*	
	8	001	*Prepaid Request*	This message does not contain any TLVs, so there is no message layout.
	9	010	*Prepaid Notify*	This message does not contain any TLVs, so there is no message layout.
5 (R3 Mobility)	1	001	*Anchor_DPF_HO_Req*	Table 4-118, Table 4-138
	2	100	*Anchor_DPF_HO_Trigger*	Table 4-119
	3	010	*Anchor_DPF_HO_Rsp*	Table 4-120
	4	001	*Anchor_DPF_Relocate_Req*	Table 4-123
	5	010	*Anchor_DPF_Relocate_Rsp*	Table 4-126
	6	001	*FA_Register_Req*	Table 4-124
	7	010	*FA_Register_Rsp*	Table 4-125
	8	001	*FA_Revoke_Req*	Table 4-129
	9	010	*FA_Revoke_Rsp*	Table 4-130
	10	001	*Anchor_DPF_Release_Req*	This message does not contain any TLVs, so there is no message layout.
	11	001	*Relocation_Ready_Req*	This message does not contain any TLVs, so there is no message layout.
	12	010	*Relocation_Ready_Rsp*	This message does not contain any TLVs, so there is no message layout.
6 (Paging)	1	100	*Paging_Announce*	Table 4-169, Table 4-170
	2	001	*Delete_MS_Entry_Req*	This message does not contain any TLVs, so there is no message layout.
	3	100	*PC_Relocation_Ind*	Table 4-163
	4	011	*PC_Relocation_Ack*	Table 4-164

Function Type	Msg Type	OP ID	Message	Message Layout
	5	010	*Delete_MS_Entry_Rsp*	This message does not contain any TLVs, so there is no message layout.
	6	100	*Anchor_PC_Ind*	Table 4-188
	7	011	*Anchor_PC_Ack*	Table 4-189
7 (RRM)	1	001	R6 *PHY_Parameters_Req (used in Release 1.0 only)*	
	2	010	R6 *PHY_Parameters_Rpt (used in Release 1.0 only)*	
	3	001	*Spare_Capacity_Req*	Table 4-149
	4	010 (for the report send for *Spare_Capacity_Req* message) and 100 (for periodic or event-driven reporting without request)	*Spare_Capacity_Rpt*	Table 4-150
	5	100	R6 *Neighbor_BS_Resource _Status_Update (used in Release 1.0 only)*	
	6	001	*Radio_Config_Update_ Req*	Table 4-151
	7	010 (for the report send for *Radio_Config_Updat e_Req* message) and 100 (Report sent as an Indication and waiting for *Radio_Config_Updat e_Ack* message)	*Radio_Config_Update_ Rpt*	Table 4-152
	8	011 for the 3-way Handshake and 010 in case of 2-way transaction	*Radio_Config_Update_ Ack*	Table 4-153
8 (Authentication	1	100	*AR_EAP_Start*	Table 4-10
	2	100	*AR_EAP_Transfer*	Table 4-11

Function Type	Msg Type	OP ID	Message	Message Layout
Relay)	3	001	*Bulk Interim Update*	Table 4-36
	4	010	*Bulk Interim Update_Ack*	This message does not contain any TLVs, so there is no message layout.
9 (MS State)	1	001	*MS_PreAttachment_Req*	Table 4-44
	2	010	*MS_PreAttachment_Rsp*	Table 4-45
	3	011	*MS_PreAttachment_Ack*	Table 4-46
	4	001	*MS_Attachment_Req*	Table 4-48
	5	010	*MS_Attachment_Rsp*	Table 4-49
	6	011	*MS_Attachment_Ack*	Table 4-50
	7	001	*Key_Change_Directive*	Table 4-12
	8	001	*Key_Change_Cnf*	Table 4-13
	9	010	*Key_Change_Ack*	Table 4-14
	10	001	*Relocation_Complete_Req*	This message does not contain any TLVs, so there is no message layout.
	11	010	*Relocation_Complete_Rsp*	This message does not contain any TLVs, so there is no message layout.
	12	011	*Relocation_Complete_Ack*	This message does not contain any TLVs, so there is no message layout.
	13	001	*Relocation_Notify*	Table 4-15,
	14	001	*Relocation_Req*	Table 4-20
	15	010	*Relocation_Rsp*	Table 4-21
	16	001	*NetExit_MS_State_Change_Req*	Table 4-54
	17	010	*NetExit_MS_State_Change_Rsp*	Table 4-55
	18	010	*Relocation_Notify_Rsp*	Table 4-16
	19	001	*Relocation_Trigger*	Table 4-204
10 IM Operations	1	001	*IM_Entry_State_Change_Req*	Table 4-37, Table 4-187, Table 4-190
	2	010	*IM_Entry_State_Change_Rsp*	Note: SBC Context, REG Context, SA Descriptor and SF Info. are only transmitted by Relay PC to Anchor PC. Table 4-191

Function Type	Msg Type	OP ID	Message	Message Layout
	3	011	*IM_Entry_State_Change_Ack*	Table 4-192
	4	001	*IM_Exit_State_Change_Req*	Table 4-175, Table 4-178
	5	010	*IM_Exit_State_Change_Rsp*	Table 4-34, Table 4-176, Table 4-179
	6	001	*Initiate_Paging_Req*	Table 4-167
	7	010	*Initiate_Paging_Rsp*	Table 4-168
	8	001	*LU_Req*	Table 4-158
	9	010	*LU_Rsp*	Table 4-159
	10	011	*LU_Cnf*	Table 4-160
11 Accounting	1	001	*Hotlining_Req*	Table 4-42
	2	010	*Hotlining_Rsp*	Table 4-43
14 R4R6R8_Capability	1	001	*Capability_Req*	Table 4-195
	2	010	*Capability_Rsp*	Table 4-196
	3	011	*Capability_Ack*	Table 4-197
15 General (not MS specific)	1	001	*Keep-alive_Req*	Table 4-198
	2	010	*Keep-alive_Rsp*	Table 4-199

5.3 TLV Definitions

5.3.1 TLV Format

The format of TLV appears below:

<table>
<tr><td>00</td><td>01</td><td></td><td></td><td></td><td></td><td></td><td>07</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>15</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>23</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>31</td></tr>
<tr><td>T C</td><td colspan="15">Type</td><td colspan="16">Length</td></tr>
<tr><td colspan="32">Value (actual number of octets in the Value Field is specified in the value of the Length Field)</td></tr>
</table>

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

Type	1
Length in octets	1
Value	Enumerator. The values are: • 0x00 = accept • 0x01 = reject All other values are Reserved.
Description	Indicates Accept/Reject of the corresponding request.
Parent TLV(s)	None

5.3.2.2 Accounting Extension

Type	2
Length in octets	Variable
Value	String
Description	This parameter indicates information relevant for accounting. The operation and the application content provider determine the format and value of the Accounting Extension.
Parent TLV	SF Info

5.3.2.3 Action Code

Type	3
Length in octets	2
Value	Enumerator. The values are: • 0x0000 = Deregister MS/AMS. MS/AMS SHALL immediately terminate service with the BS/ABS and should attempt network entry at another BS/ABS; • 0x0001 = Suspend all MS/AMS traffic including control traffic. MS/AMS SHALL listen to the current BS/ABS but SHALL not transmit until an RES-CMD/AAI-RES-CMD message or DREG-CMD/AAI-DREG-RSP with Action Code 02 or 03 is received; • 0x0002 = Suspend user traffic (transport connections). MS/AMS SHALL listen to the current BS/ABS but only transmit on the Basic and Primary Management Connections (in particular, in Mzone of ABS Basic and Primary Management connections are not defined separately, but both connections are merged into the management connection) ; • 0x0003 = Resume traffic. MS/AMS SHALL return to normal operation and may transmit on any of its active connections. • 0x0005 = MS/AMS SHALL be put into idle mode. • 0xfffe = Initial Authentication Failure. MS/AMS SHALL be sent the RNG-RSP/AAI-RNG-RSP with Ranging Result Code = Abort by the BS/ABS. • 0xffff = MS/AMS SHALL be sent the RES-CMD/AAI-RES-CMD by the BS/ABS. The MS/AMS will reload all configuration information and do initial network entry. All other values are Reserved.
Description	Indicates the action code to be used by BS/ABS in the DREG-CMD/AAI-DREG-RSP. Action Code TLV is used only in the messages directed to a BS/ABS.
Message Primitives That Use This TLV	Path Control messages (*Path_Dereg_Req*), MS State Change messages.

5.3.2.4 Action Time

Type	4
Length in octets	4
Value	32-bit unsigned integer.
Description	For HO, this value indicates the radio frame in which the Target BS/ABS allocates a dedicated transmission opportunity for RNG-REQ message to be transmitted by the MS/AMS using Fast Ranging IE. This value is defined in absolute number of radio frames.
Parent TLV(s)	BS Info

5.3.2.5 AK

Type	5
Length in octets	20
Value	160-bit AK Value.
Description	AK is derived from the PMK at the NAS.
Parent TLV(s)	AK Context

5.3.2.6 AK Context

Type	6	
Length in octets	Variable but not less than 10	
Value	Compound	
Description	Contains AK Context from Authenticator.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	AK	M
	AK ID	M
	AK Lifetime	M
	AK SN	M
	CMAC_KEY_COUNT	M
Parent TLV(s)	BS Info	

5.3.2.7 AK ID

Type	7
Length in octets	8
Value	64-bit AK ID Value.
Description	Identifies the AK that is used for protecting the message.
Parent TLV(s)	AK Context

5.3.2.8 AK Lifetime

Type	8
Length in octets	4
Value	32-bit AK Lifetime value in seconds.
Description	The time period during which the AK will be valid.
Parent TLV(s)	AK Context

5.3.2.9 AK SN

Type	9
Length in octets	1
Value	The field is coded as follows: 4-bit Reserved | 4-bit AK SN.
Description	The Sequence number of root keys (PMK) for the AK.
Parent TLV(s)	AK Context

5.3.2.10 Anchor ASN GW ID

Type	10
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 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.
Description	Unique identifier for the Anchor GW / Anchor Data Path Function.
Parent TLV(s)	MS Info

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	

5.3.2.12 Anchor PC ID

Type	12
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	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.
Description	Unique identifier for the Paging Controller network entity, which administers paging activity for the MS/AMS while in Idle Mode and retains MS service and operational information.
Parent TLV(s)	Paging Information, IDLE Mode Info.

5.3.2.13 Anchor PC Relocation Destination

Exists if relocation is requested.

Type	13
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	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.
Description	Network identifier for a new (target) Anchor Paging Controller network entity, which administers paging activity for the MS/AMS while in Idle Mode and retains MS service and operational information.
Parent TLV(s)	Paging Information

5.3.2.14 Anchor PC Relocation Request Response

Exists if relocation is requested.

Type	14
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Accept • 0x01 = Refuse All other values are Reserved.
Description	Indicates Accept/Reject of the corresponding request.
Parent TLV(s)	Paging Information

5.3.2.15 Associated PHSI

Type	15
Length in octets	1
Value	8-bit unsigned integer.
Description	The Associated PHSI value. It SHALL be equal to the PHSI value of the corresponding PHS Rule.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.16 FA Revoke Reason

Type	16
Length in octets	1
Value	Enumerator. The values are: • 0x00 = DHCP Release • 0x01 = DHCP expiry • 0x02 = FA initiated release • 0x03 = HA initiated release All other values are Reserved.
Description	Indicates the FA Revoke Reason.
Message Primitives That Use This TLV	FA Revoke Req

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
	PKMv2/PKMv3 Message Code	M
Message Primitives That Use This TLV	Key_Change_Directive	

5.3.2.18 Authentication Result

Type	18
Length in octets	1
Value	• Enumerator. The values are:0x00 = Success • 0x01 = Failure All other values are Reserved.
Description	This parameter indicates to BS/ABS the results of EAP authentication process.
Parent TLV(s)	Authentication Complete, MS Info

5.3.2.19 Authenticator ID

Type	19
Length in octets	Variable (could be of three fixed sizes: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 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.
Description	Unique identifier of MS/AMS's Anchor Authenticator.
Parent TLV(s)	MS Info

5.3.2.20 RRQ

Type	20
Length in octets	Variable
Value	Same as defined in [49] including IP/UDP headers.
Description	MIP Register Request message defined in [49].
Parent TLV(s)	FA_Register_Req

Note [a]: Used only during HO/ Idle Mode entry/exit operations.

5.3.2.21 Authorization Policy Support

Type	21
Length in octets	1
Value	8-bit Bitmask coded as follows: • Bit #0 = RSA-based authorization at the initial network entry • Bit #1 = EAP-based authorization at the initial network entry • Bit #2 = Authenticated EAP-based authorization at the initial network entry • Bit #4 = RSA-based authorization at reentry • Bit #5 = EAP-based authorization at reentry • Bit #6 = Authenticated EAP-based authorization at reentry All other bits are Reserved.
Description	This parameter is used to indicate authentication mode. In MS Security History TLV, it indicates the capability negotiated between ASN and MS/AMS. Refer to 11.8.4.2 Authorization policy support in 802.16e/m.
Parent TLV	MS Security History, Security Negotiation Parameters

5.3.2.22 Available Radio Resource DL

Type	22
Length in octets	1
Value	8-bit unsigned integer: • 0x00 = 0% • 0x01 = 1%, • ..., • 0x64 = 100% All other values are Reserved.
Description	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 *Spare_Capacity_Req* if provided; if omitted, the BS/ABS SHALL apply a default value.
Parent TLV(s)	RRM BS Info

5.3.2.23 Available Radio Resource UL

Type	23
Length in octets	1
Value	8-bit unsigned integer: • 0x00 = 0% • 0x01 = 1%, • ..., • 0x64 = 100% All other values are Reserved.
Description	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 *Spare_Capacity_Req* if provided; if omitted, the BS/ABS SHALL apply a default value.
Parent TLV(s)	RRM BS Info

5.3.2.24 BE Data Delivery Service

<table>
<tr><th>Type</th><td colspan="2">24</td></tr>
<tr><th>Length in octets</th><td colspan="2">Variable</td></tr>
<tr><th>Value</th><td colspan="2">Compound</td></tr>
<tr><th>Description</th><td colspan="2">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.</td></tr>
<tr><th rowspan="4">Elements (Sub-TLVs)</th><th>TLV Name</th><th>M/O</th></tr>
<tr><td>Maximum Sustained Traffic Rate</td><td>O</td></tr>
<tr><td>Traffic Priority</td><td>O (if omitted means Traffic Priority = 0)</td></tr>
<tr><td>Request/Transmission Policy</td><td>O [a]</td></tr>
<tr><th>Parent TLV</th><td colspan="2">QoS Parameters</td></tr>
</table>

Note: [a] – Used during Service flow creation, HO/ Idle Mode entry/ exit operations.

5.3.2.25 BS ID

Type	25
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 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. Note: The Identifier sent to the anchor authenticator should be the 6-octet 802.16 BS ID, used by the anchor authenticator for AK generation. If the 6-octet 802.16 BS ID is not provided, the anchor authenticator shall be able to map the IP address (either the 4-octet IPv4 Address, or the 16-octet IPv6 Address) to the 6-octet 802.16 BS ID. The mapping mechanism is out of scope of this specification.
Description	Unique BS Identifier, referring to a single sector with a single frequency assignment.
Parent TLV(s)	BS Info, RRM BS Info

5.3.2.26 BS Info

Type	26	
Length in octets	Variable	
Value		
Description	Description of BS/ABS.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	BS ID	M
	Serving/Target Indicator	O[28]
	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
	Data Integrity Capability	O
	Spare Capacity Indicator	O
	Service Level Prediction	O
	Preamble Index / Sub-channel Index	O
	SF Info	O (Note 2)
	Action Time	O
	Time Stamp	O
	BS HO RSP Code	O
	AK Context	O (Note 1)
	BS Location	O
	Reattachment Zone	O
	Data Integrity Method	O
	IP Address of Requesting BS	O

[28] Serving/Target Indicator is conditionally mandatory. See tables in section 3.2.

Message Primitives That Use This TLV	Every Message

Note: HO ID is defined in the IEEE 802.16e spec.

1)AK Context SHALL be included as sub-TLV of BS Info in the following messages:

a. Key_Change_Directive Message in order to transfer the new security context (AK Context) to BS/ABS and trigger the PKMv2/v3 3-WHS process between the BS/ABS and the MS/AMS.

b. Context_Rpt from authenticator ASN to Target ASN.

c. May be included in HO-Req message.

2)One or more instances may occur.

5.3.2.27 BS-originated EAP-Start Flag

Type	27
Length in octets	0
Value	N/A
Description	Flag indicating that *AR_EAP_Start* message is originated by a BS/ABS (without receiving PKMv2 EAP-Start/PKMv3 Reauth-Request from an MS/AMS). A BS/ABS may use *AR_EAP_Start* with this flag to instigate reauthentication process when MS security context in BS/ABS is going to expire.
Parent TLV	MS Info

5.3.2.28 Care-of Address (CoA)

Type	28
Length in octets	4
Value	Care-of Address (CoA) of the MS/AMS.
Description	
Parent TLV(s)	MIP4 Info

5.3.2.29 CID/MCID

Type	29
Length in octets	2
Value	16-bit unsigned integer.
Description	CID/MCID definition as per 802.16e.
Parent TLV(s)	SF Info

5.3.2.30 Classification Rule Index

Type	30
Length in octets	2
Value	16-bit unsigned integer.
Description	This TLV defines the index assigned to this classification rule: • The index is unique per service flow.
Parent TLV(s)	Packet Classification Rule / Media Flow Description

5.3.2.31 Classification Rule Action

Type	31
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Add Classification Rule, • 0x01 = Replace Classification Rule, • 0x02 = Delete Classification Rule. All other values are Reserved.
Description	Add, replace or delete the classification Rule for the classification of a specific service flow.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.32 Classification Rule Priority

Type	32
Length in octets	1
Value	8-bit unsigned integer.
Description	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.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.33 Vendor ID

Type	33
Length in octets	3
Value	24-bit vendor-specific Organization Unique Identifier (OUI)
Description	Vendor Identification of the Network Element Vendor or Network Provider
Message Primitives That Use This TLV	Capability_Req, Capability_Rsp

5.3.2.34 CMAC_KEY_COUNT

Type	34
Length in octets	2
Value	Unsigned 16-bit integer.
Description	Value of the Entry Counter that is used to guarantee freshness of computed CMAC_KEY_* with every entry and provide replay protection. Upon initial network entry, count is reset to 0 in the MS/AMS and Serving BS/ABS, and to 1 in the Authenticator.
Parent TLV(s)	AK Context
	MS Info

5.3.2.35 Combined Resources Required

Type	35
Length in octets	2
Value	Enumerator. The values are: • 0x0000 = Not combined; • 0x0001 =Combined; All other values are Reserved.
Description	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, If the CS Type TLV indicates "All CS Types," then this TLV applies to all pre-provisioned SFs for the MS. Absence of this TLV is interpreted as if the TLV's value is set to 0x0000.
Parent TLV	Combined Resource Indicator

5.3.2.36 Context Purpose Indicator

Type	36
Length in octets	4
Value	32-bit Bitmask. • Bit #0 = MS/AMS AK Context. • Bit #1 = MS/AMS Network Context • Bit #2 = MS/AMS MAC Context • Bit #3 = MS/AMS Authorization Context • Bit #4 = Anchor MM Context • Bit #5 = Accounting context • Bit #6 = MS Security History • Bit #7 = SA Context • Bit #8 = MN-FA key context • Bit #9 = FA-HA key context • Bit #10 = DHCP-Relay-Info • Bit #11 = Security Context Delivery • Bit #12 = MIP6 handover successful • Bit #13 = Online Accounting context • Bit #14 = Offline Accounting context All other bits are Reserved.

Description	Indicates the type of context to be delivered: • Setting Bit #0 requests delivering AK Context associated with a particular MS/AMS. • 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/AMS and known to the responder. • Setting Bit#2 requests delivery of MAC Context associated with a particular MS/AMS that is available in BS/ABS. This includes REG Context, SBC Context and PKMv2/v3 context. • Setting Bit#3 requests delivery of service authorization and policy context (e.g., authorization code) associated with a particular MS/AMS. • Setting Bit#4 requests delivery of Anchor MM Context associated with a particular MS. • Setting Bit#5 requests delivery of Accounting provisioning info • Setting Bit#6 requests delivery of MS Security History • Setting Bit#7 requests SA Context. This is included based on the bits set in the Idle Mode Retain Information TLV from the MS/AMS and if cached in the BS/ABS apriori. • Setting Bit#7 requests delivery of MIP4 Security Info TLV with MN-FA key context. • Setting Bit#9 requests delivery of MIP4 Security Info TLV with FA-HA key context. • Setting Bit#10 requests delivery of DHCP relay information. • Setting Bit#11 requests delivery of the security context. • 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. • Setting Bit#13 requests delivery of Online Accounting context/ quota(s). • Setting Bit#14 requests delivery of Offline Accounting context.
Message Primitives That Use This TLV	Context Delivery messages.

5.3.2.37 Correlation ID

Type	37
Length in octets	4
Value	32-bit unsigned integer.
Description	Indicates correlation between Service Flows. Service Flows with the same Correlation ID are assumed to be related on higher layers and may be treated with common policy. Correlation ID may be associated with SDFID on R3, or allocated locally at the ASN.
Parent TLV(s)	SF Info

5.3.2.38 Cryptographic Suite

Type	38
Length in octets	4
Value	Enumerator. The values are: • 0x00000 = No data encryption, no data authentication & 3-DES, 128 • 0x010001 = CBC-Mode 56-bit DES, no data authentication & 3-DES, 128 • 0x000002 = No data encryption, no data authentication & RSA, 1024 • 0x010002 = CBC-Mode 56-bit DES, no data authentication & RSA, 1024 • 0x020103 = CCM-Mode 128-bit AES, CCM-Mode, 128-bit, ECB mode AES with 128-bit key • 0x020104 = CCM-Mode 128bits AES, CCM-Mode, AES Key Wrap with 128-bit key • 0x030003 = CBC-Mode 128-bit AES, no data authentication, ECB mode AES with 128-bit key • 0x800003 = MBS CTR Mode 128 bits AES, no data authentication, AES ECB mode with 128-bit key • 0x800004 = MBS CTR mode 128 bits AES, no data authentication, AES Key Wrap with 128-bit key All other values are Reserved.
Description	Indicates cryptographic suites allowed.
Parent TLV(s)	SA Descriptor

5.3.2.39 CS Type

Type	39
Length in octets	1
Value	Enumerator. The values are: • 0x00 = All CS Types • 0x01 = Packet, IPv4 • 0x02 = Packet, IPv6 • 0x03 = Packet, 802.3 • 0x04 = void • 0x05 = void • 0x06 = void All other values are Reserved.
Description	Indicates type of convergence layer between MS/AMS and BS/ABS.
Parent TLV(s)	SF Info, Combined Resource Indicator

5.3.2.40 Data Integrity

Type	40
Length in octets	1
Value	Enumerator. The values are: • 0x00 = No recommendation • 0x01 = Data integrity requested • 0x02 = Data delay jitter sensitive All other values are Reserved.
Description	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.
Parent TLV	QoS Parameters

5.3.2.41 PMIP-Authenticated-Network-Identity

Type	41
Length in octets	Variable up to 256 octets
Value	ASCII String
Description	PMIP Network Access Identifier character string
Parent TLV(s)	MS Security History, MS Authorization Context, MIP4 Security Info
Message Primitives That Use This TLV	Context Request

5.3.2.42 Data Path Encapsulation Type

Type	42
Length in octets	1
Value	Enumerator. The values are: • 0x01 = GRE • 0x02 =VOID • 0x03 = VOID All other values are Reserved.
Description	Data Path Type.
Parent TLV	Data Path Info

5.3.2.43 Void

5.3.2.44 Data Path ID

Type	44
Length in octets	4
Value	Data Path Identifier (e.g., GRE Key).
Description	Identifier for a data path.
Parent TLV	Data Path Info

5.3.2.45 Data Path Info

Type	45	
Length in octets	Variable	
Value	Compound	
Description	Data Path Description.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Data Path ID	O[Note1]
	Data Path Encapsulation Type	O
	Data Path Type	O
	Tunnel Endpoint	O
	Switching Data Path ID	O[Note1]
Parent TLV	SF Info (for per SF Data Path)	

Note1: At least Data Path ID or Switching Data Path ID shall be included.Void

5.3.2.46 Void

5.3.2.47 Data Path Type

Type	47
Length in octets	1
Value	Enumerator. The values are: • 0x01 = Type1 • 0x02 = Type2 All other values are Reserved.
Description	Distinguishes between Type 1 and Type 2 datapaths.
Parent TLV	Data Path Info

1 ### 5.3.2.48 DCD/UCD Configuration Change Count

Type	48
Length in octets	1
Value	8-bit integer: • Bits #0…3 = The 4 LSBs of the BS's current DCD configuration change count; • Bits #4…7 = The 4 LSBs of the BS's current UCD configuration change count.
Description	This includes the 4 LSBs of the BS's current DCD and UCD configuration change count figures
Parent TLV(s)	RRM BS Info

2 ### 5.3.2.49 DCD Setting

Type	49
Length in octets	Variable
Value	Compound, as specified in [802.16e-2005], section 11.1.7.
Description	This is an IEEE802.16e-2005 defined TLV. The DCD_settings is a TLV value that encapsulates a DCD message (excluding the generic MAC header and CRC) that may be transmitted in the advertised BS downlink channel. This information is intended to enable fast synchronization of the MS with the advertised BS downlink. The DCD 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. See [802.16e-2005], section 11.1.7.
Parent TLV(s)	RRM BS Info

5.3.2.50 ODFMA Parameters Sets

Type	50
Length in octets	1
Value	8-bit bitmask
Description	Identifies the profile of the capabilities of the MS negotiated during SBC handshake • Bit#0 = Support OFDMA PHY parameter set A • Bit#1 = Support OFDMA PHY parameter set B • Bit#2-#4 = HARQ parameters set – 0b000 = HARQ set 1 – 0b001 = HARQ set 2 – 0b010 = HARQ set 3 – 0b011 = HARQ set 4 – 0b100 = HARQ set 5 – 0b101-0b111 = Reserved • Bit#5 = Support OFDMA MAC parameters set A • Bit#6 = Support OFDMA MAC parameters set B • Bit#7 = Reserved Note: Bit#0 and #1 SHALL not be set to 1 together. Bit#5 and #6 SHALL not be set to 1 together.
Parent TLV	SBC Context

5.3.2.51 DHCP Key

Type	51
Length in octets	20
Value	160-bit unsigned integer.
Description	Key used to calculate and authenticate messages between the DHCP relay in the ASN and DHCP server in the CSN, as per [66]. This TLV SHALL be included in the *Context_Rpt* message (as part of DHCP Relay Info TLV) if Context Purpose Indicator TLV was set to DHCP-Relay-Info.
Parent TLV(s)	DHCP Relay Info

5.3.2.52 DHCP Key ID

Type	52
Length in octets	4
Value	32-bit unsigned integer.
Description	Key ID associated with the key used to compute authentication suboption as per [66]. This TLV SHALL be included in the *Context_Rpt* message (as part of DHCP Relay Info TLV) if DHCP Key TLV is included.
Parent TLV(s)	DHCP Relay Info

5.3.2.53 DHCP Key Lifetime

Type	53
Length in octets	4
Value	32-bit unsigned integer.
Description	The remaining lifetime in seconds of the DHCP key. This TLV SHALL be included in the *Context_Rpt* message (as part of DHCP Relay Info TLV) if DHCP Key TLV is included.
Parent TLV(s)	DHCP Relay Info

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	

5.3.2.55 DHCP Relay Address

Type	55
Length in octets	Variable (either 4 or 16 bytes)
Value	IPv4 or IPv6 address.
Description	DHCP relay's IPv4 or IPv6 address facing the DHCP server. This TLV SHALL be included in the *Context_Req* message (as part of DHCP Relay Info TLV) if Context Purpose Indicator TLV is set to DHCP-Relay-Info.
Parent TLV(s)	DHCP Relay Info

5.3.2.56 DHCP Relay Info

Type	56	
Length in octets	Variable	
Value	Compound	
Description	Information about the DHCP Relay. This TLV SHALL be included in the *Context_Req* and *Context_Rpt* messages if Context Purpose Indicator TLV is set to DHCP-Relay-Info.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	DHCP Server Address	O
	DHCP Relay Address	O
	DHCP Key	O
	DHCP Key ID	O
	DHCP Key Lifetime	O
Parent TLV(s)	*MS Info.*	

5.3.2.57 DHCP Server Address

Type	57
Length in octets	Variable (either 4 or 16)
Value	IPv4 or IPv6 address.
Description	IPv4 or IPv6 address of the DHCP server. This TLV SHALL be included in the *Context_Rpt* 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.
Parent TLV(s)	DHCP Relay Info and DHCP Server List

5.3.2.58 DHCP Server List

Type	58	
Length in octets	Variable	
Value	Compound	
Description	List of DHCP servers.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	DHCP Server Address	O
Parent TLV(s)	Anchor MM Context	

5.3.2.59 Direction

Type	59
Length in octets	2
Value	Enumerator. The values are: • 0x0000 = For Uplink • 0x0001 = For Downlink All other values are Reserved.
Description	Describes the unidirectional Service Flow direction (i.e., UL or DL).
Parent TLV	SF Info, HARQ Context

5.3.2.60 DL PHY Quality Info

Type	60
Length in octets	4
Value	32-bit integer encoding 8-bit DL RSSI Mean, 8-bit DL RSSI Std, 8-bit DL CINR Mean, 8-bit DL CINR Std.
Description	
Parent TLV	BS Info, RRM BS-MS PHY Quality Info

5.3.2.61 DL PHY Service Level

Type	61
Length in octets	4
Value	32-bit integer representing DL PSL.
Description	
Parent TLV	RRM BS-MS PHY Quality Info

5.3.2.62 EAP Payload

Type	62
Length in octets	Variable
Value	EAP Payload (for EAP over R6 Authentication Relay).
Description	EAP Messages.
Message Primitives That Use This TLV	EAP Relay messages

5.3.2.63 Void

5.3.2.64 ERT-VR Data Delivery Service

Type	64	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains the QoS parameters relevant for ERT-VR Data Delivery Service. If included in QoS Parameters, it implies ertPS Scheduling Service for UL connections.	
Elements (Sub-TLVs)	**TLV Name**	**M/O Flag**
	Minimum Reserved Traffic Rate	M
	Maximum Latency	M
	Tolerated Jitter	O (omission means jitter equal to maximum latency)
	Unsolicited Grant Interval	O
	Traffic Priority	O (if omitted means Traffic Priority = 0)
	Maximum Sustained Traffic Rate	O (if absent defaulting to Minimum Reserved Traffic Rate)
	Request/Transmission Policy	O (see Note [a])
	Maximum Traffic Burst	O
Parent TLV	QoS Parameters	

Note [a]: Used during Service flow creation, HO/ Idle Mode entry/exit operations.

5.3.2.65 PPAC

Type	65	
Length in octets	Variable	
Value	Compound	
Description	The PrepaidAccountingCapability (PPAC) TLV is sent by a prepaid capable ASN entity and is used to describe the prepaid capabilities of the ASN.	
Elements (Sub-TLVs)	**TLV Name**	**M/O Flag**
	AvailableInClient	M
Message Primitives that use this TLV	Relocation_Complete_Rsp, Anchor_DPF_HO_Trigger, Anchor_DPF_HO_Req	

5.3.2.66 FA-HA Key

Type	66
Length in octets	20
Value	160-bit unsigned integer.
Description	Using FA-HA key to calculate and authenticate FA-HA-AE, integrity can be protected between HA and FA.
Parent TLV(s)	MIP4 Security Info

5.3.2.67 FA-HA Key Lifetime

Type	67
Length in octets	4
Value	32-bit unsigned integer.
Description	Time of FA-HA key remaining valid.
Message Primitives That Use This TLV	MIP4 Security Info

5.3.2.68 FA-HA Key SPI

Type	68
Length in octets	4
Value	32-bit unsigned integer.
Description	Key ID of FA-HA key. It should be equal to the SPI (Key ID) of HA-RK.
Message Primitives That Use This TLV	MIP4 Security Info

5.3.2.69 Failure Indication

Type	69
Length in octets	1 byte
Value	Enumerator. The values are: • 0x00 = Unspecified Error Error Codes: 0x01-0x0F Message Header Failure Codes • 0x01 = Protocol Version not understood (note 1) • 0x02 = Unrecognized Function Type • 0x03 = Invalid Message Type • 0x04 = Unknown MSID • 0x05 = Transaction Failure • 0x06 = Source Identifier unknown or inconsistent with the IP source address • 0x07 = Destination unknown • 0x08 = Invalid Message Header

	• 0x09 = Invalid OP ID • 0x0A = Destination Identifier missing or erroneous • 0x0B = Source Identifier TLV missing or erroneous • 0x0C = Message type unknown or inopportune • 0x0D = Unresolved error • 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". Error Codes: 0x10-0x1F General Message Body Failure Codes • 0x10 = Invalid message format • 0x11 = Mandatory TLV missing • 0x12 = TLV Value Invalid • 0x13 = Unsupported Options • 0x14 = TLV Unknown • 0x15 = TLV Unexpected • 0x16 = TLV parsing error • 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". Error Codes: 0x20-0x2F Message Generic Failure Codes • 0x20 = Timer expired without response • 0x21 = BSID out of service • 0x22 = Unknown BSID • 0x23 = BSID Unreachable • 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 ". Error Codes: 0x30-0x7F Message-specific Failure Codes • 0x30 = Requested Context Unavailable • 0x31 = Authorization Failure • 0x32 = Registration Failure • 0x33 = No Resources • 0x34 = Failure by rejection of MS/AMS • 0x35 = Authenticator relocated • 0x36 = Does not support periodic reporting of RRM messages • 0x37 = Location Update Failure • 0x38 = Idle Mode Authorization Failure • 0x39 = Target BS/ABS doesn’t support this HO Type • 0x3A = Insufficient Target BS/ABS airlink resource • 0x3B = Target BS/ABS CPU overload • 0x3C = Out of MS Reattachment Zone • 0x3D = Locked State • 0x3E = Failed to allocate CRID

	- 0x3FE-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" (To be updated with sub section team specific error handling) 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". 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".
Description	Indicates the reason for failure of a previous message The sender SHALL include the Failure Indication TLV in the *first free position after the header* (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 *first free position after the header* (see section 3.5.2) of each Error Response or Error Reflection message (see section 3.5.2).
Parent TLV	None
Message Primitives That Use This TLV	Any message on R6/R4/R8 that is used for failure reporting.

Note 1: This value might be used by legacy entities to indicate that a message with Protocol Version different from 1 has been received. The value should be blocked for any other use in protocol version 1.

5.3.2.70 Target FA IP Address

Type	70
Length in octets	4
Value	IP address of the entity which containing an FA function.
Description	
Parent TLV(s)	MIP4 Info

5.3.2.71 FA Relocation Indication

Type	71
Length in octets	1
Value	Enumerator. The values are: - 0x00 = Success - 0x01 = Failure All other values are Reserved.
Description	Indicates the FA relocation process. It SHALL be set to indicate "Success" if FA relocation has been Successfully completed with authenticator relocation, otherwise it should indicate "Failure".
Parent TLV(s)	MS Info

5.3.2.72 Full DCD Setting

Type	72
Length in octets	Variable
Value	Compound, as specified in [802.16e-2005], section 11.1.7.
Description	This is an IEEE802.16e-2005 defined TLV. The DCD_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/AMS with the advertised BS downlink. See [802.16e-2005], section 11.1.7.
Parent TLV(s)	RRM BS Info

5.3.2.73 Full UCD Setting

Type	73
Length in octets	Variable
Value	Compound, as specified in [802.16e-2005], section 11.1.7.
Description	This is an IEEE802.16e-2005 defined TLV. The UCD_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/AMS with the advertised BS downlink. See [802.16e-2005], section 11.1.7.
Parent TLV(s)	RRM BS Info

5.3.2.74 Global Service Class Name

Type	74
Length in octets	6
Value	Global Service Class Name as defined in IEEE802.16e/m.
Description	Provides an authorized QoS parameters set in a length optimized format.
Parent TLV(s)	QoS Parameters, R3 QoS Descriptor

5.3.2.75 HA IP Address

Type	75
Length in octets	Variable (either 4 or 16)
Value	IP address of HA. The Identifier might be in format of either a 4-octet IPv4 Address or a 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	
Parent TLV(s)	MIP4 Info, MIP4 Security Info

1 5.3.2.76 HO Confirm Type

Type	76
Length in octets	1
Value	Enumerator. The values are Enumerator: • 0x00 = Confirm • 0x01 = Unconfirm • 0x02 = Cancel • 0x03 = Reject All other values are Reserved.
Description	Indicates whether one of the candidate BS/ABSs is selected as the HO target or not. Here, "Confirm " is for when the network receives an explicit indication of handover target BS/ABS from MS/AMS, "Unconfirm" for when the network fails to receive an indication from MS/AMS but network presumes possible target BS/ABSs, "Cancel" for when MS/AMS cancels the handover, and "Reject" for when MS/AMS rejects handover to one of the candidate BS/ABSs proposed by the network.
Message Primitives That use this TLV	HO_Cnf

2 5.3.2.77 Home Address (HoA)

Type	77
Length in octets	4
Value	Home Address (HoA) of the MS/AMS. In case of PMIP6 it is the IPv4 MN-HoA
Description	
Parent TLV(s)	MIP4 Info, PMIP6 Info

3 5.3.2.78 HO Process Optimization

Type	78
Length in octets	1
Value	8-bit integer representing HO Process Optimization code.
Description	
Parent TLV	BS Info, RRM BS Info

1 ### 5.3.2.79 HO Type

Type	79
Length in octets	4
Value	Enumerator. The values are: • 0x00000000 = Hard Handoff (HHO) • 0x00000001 = Fast Base Station Switching (FBSS) • 0x00000002 = Macro Diversity Handoff (MDHO) • 0x00000003 =Zone Switch Handoff All other values are Reserved.
Description	Allows communication of various handover types.
Message Primitives That Use This TLV	HO Control messages

2 ### 5.3.2.80 IDLE Mode Info

Type	80	
Length in octets	Variable	
Value	Compound	
Description	Indicates if the MS/AMS 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

Type	81
Length in octets	1
Value	
Description	Indicates which re-entry management messages SHALL be retained and managed. Encoded as in 802.16e/m.
Parent TLV(s)	Paging Information

1 ### 5.3.2.82 IP Destination Address and Mask

Type	82
Length in octets	8 (IPv4) or 32 (IPv6).
Value	An IP Destination Address/Mask pairs: (dst1, dmask).
Description	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.
Parent TLV	Packet Classification Rule / Media Flow Description

2 ### 5.3.2.83 IP Remained Time

Type	83
Length in octets	4
Value	32-bit unsigned integer.
Description	Remaining lease time for the assigned IP address, indicated in second.
Message Primitives That Use This TLV	DHCP Proxy Info

3 ### 5.3.2.84 IP Source Address and Mask

Type	84
Length in octets	8 (IPv4) or 32 (IPv6)
Value	An IP Source Address/Mask pairs: (Src1, Smask).
Description	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.
Parent TLV	Packet Classification Rule / Media Flow Description

4 ### 5.3.2.85 IP TOS/DSCP Range and Mask

Type	85
Length in octets	3
Value	The value field is structured as follows: • Octet 1: Lower Limit • Octet 2: Higher Limit • Octet 3: Mask
Description	The values of the field specify the matching parameters for the IP type of service/DSCP [IETF RFC 2474] byte range and mask. An IP packet with IP type of service (ToS) byte value “ip-tos” matches this parameter if tos-low less than or equal (ip-tos AND tos-mask) less than or equal tos-high. If this field is omitted, then comparison of the IP packet ToS byte for this entry is irrelevant.
Parent TLV	Packet Classification Rule / Media Flow Description

1 ### 5.3.2.86 Key Change Indicator

Type	86
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Success • 0x01 = Failure All other values are Reserved.
Description	The value of this parameter indicates to ASN GW/Authenticator the results of PKMv2/v3 3-way handshake process. Note, that BS/ABS indicates "Success" results when it ensures that MS/AMS had received PKMv2 SA-TEK-Response/PKMv3 Keyagreement #3 message and successfully enforced the new PMK/ AK contexts.
Parent TLV(s)	MS Info

2 ### 5.3.2.87 L-BSID

Type	87
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets).
Value	The Identifier might be in format of either 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.
Description	Unique BS Identifier, referring to a single sector with a single frequency assignment.
Message Primitives That Use This TLV	R4_Paging_Announce

3 ### 5.3.2.88 Location Update Status

Type	88
Length in octets	1
Value	Enumerator. Supported values in this release: • 0x00 = Accept All other values are Reserved.
Description	Indicates successful location update result.
Parent TLV(s)	Paging Information

5.3.2.89 AvailableInClient

Type	89
Length in octets	4
Value	4 Octet String interpreted as a bit map with the following values: • 0x00000000 = Reserved • 0x00000001 = Volume metering supported • 0x00000002 = Duration metering supported • 0x00000004 = Resource metering supported • 0x00000008 = Pools supported • 0x00000010 = Rating groups supported • 0x00000020 = Multi-Services supported • 0x00000040 = Tariff Switch supported All other values are Reserved.
Description	AvailableInClient TLV indicates the metering capabilities of the ASN and SHALL be bitmap encoded.
Parent TLV(s)	PPAC

5.3.2.90 LU Result Indicator

Type	90
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Success • 0x01 = Failure All other values are Reserved.
Description	Boolean that indicates the result of the LU operation.
Message Primitives That Use This TLV	PC_Relocation_Ind

1
5.3.2.91 Maximum Latency

Type	91
Length in octets	4
Value	32-bit integer specifies the maximum latency (in milliseconds).
Description	Time period between the reception of a packet by the BS/ABS or MS/AMS 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/ABS or MS/AMS and SHALL be guaranteed by the BS/ABS or MS/AMS. A BS/ABS or MS/AMS does not have to meet this service commitment for service flows that exceed their minimum reserved rate.
Parent TLV	• UGS Data Delivery Service • ERT-VR Data Delivery Service • RT-VR Data Delivery Service

2
5.3.2.92 Maximum Sustained Traffic Rate

Type	92
Length in octets	4
Value	32-bit integer representing rate (in bits per second).
Description	This parameter defines the peak information rate of the service. The rate is expressed in bits per second and pertains to the SDUs at the input to the system. Explicitly, this parameter does not include MAC overhead such as MAC headers or CRCs. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. If this parameter is omitted or set to zero, then there is no explicitly mandated maximum rate. This field specifies only a bound, not a guarantee that the rate is available. The algorithm for policing to this parameter is left to vendor differentiation and is outside the scope of the standard.
Parent TLV	• ERT-VR Data Delivery Service • RT-VR Data Delivery Service • NRT-VR Data Delivery Service • BE Data Delivery Service • UGS Data Delivery Service • R3 Qos Descriptor

5.3.2.93 Maximum Traffic Burst

Type	93
Length in octets	4
Value	32-bit integer representing burst size (in bytes).
Description	This parameter defines the maximum burst size that SHALL be accommodated for the service. Since the physical speed of ingress/egress ports, the air interface, and the backhaul will in general be greater than the maximum sustained traffic rate parameter for a service, this parameter describes the maximum continuous burst the system should accommodate for the service assuming the service is not currently using any of its available resources.
Parent TLV	• ERT-VR Data Delivery Service • RT-VR Data Delivery Service • NRT-VR Data Delivery Service • R3 QoS Descriptor

5.3.2.94 Media Flow Type

Type	94
Length in octets	1
Value	Enumerator. The values are: • 0x01 = Voice over IP • 0x02 = Robust Browser • 0x03 = Secure Browser/ VPN • 0x04 = Streaming video on demand • 0x05 = Streaming live TV • 0x06 = Music and Photo Download • 0x07 = Multi-player gaming • 0x08 = Location-based services • 0x09 = Text and Audio Books with Graphics • 0x0A = Video Conversation • 0x0B = Message • 0x0C = Control • 0x0D = Data All other values are Reserved.
Description	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
Parent TLV	QoS Parameters

5.3.2.95 Minimum Reserved Traffic Rate

Type	95
Length in octets	4
Value	32-bit unsigned integer representing rate (in bits per second).
Description	This parameter specifies the minimum rate reserved for this service flow. The rate is expressed in bits per second and specifies the minimum amount of data to be transported on behalf of the service flow when averaged over time. The specified rate SHALL only be honored when sufficient data is available for scheduling. When insufficient data exists, the requirement imposed by this parameter SHALL be satisfied by assuring the available data is transmitted as soon as possible.
Parent TLV	• UGS Data Delivery Service • ERT-VR Data Delivery Service • RT-VR Data Delivery Service • NRT-VR Data Delivery Service • R3 Qos Descriptor

5.3.2.96 MIP4 Info

Type	96	
Length in octets	Variable	
Value	Compound	
Description	MIP4 Information about the MS/AMS.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	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
Parent TLV(s)	Anchor MM Context, PMIP4 Context	

5.3.2.97 RRP

Type	97
Length in octets	variable
Value	Same as defined in [49] including IP/UDP headers.
Description	MIP Register Response message defined in [49].
Message Primitives That Use This TLV	FA_Register_Rsp

5.3.2.98 MN-FA Key

Type	98
Length in octets	20
Value	160-bit unsigned integer.
Description	Using MN-FA key to calculate and authenticate MN-FA-AE, integrity can be protected between MN and FA.
Parent TLV(s)	MIP4 Security Info

5.3.2.99 MN-FA SPI

Type	99
Length in octets	4
Value	32-bit unsigned integer.
Description	Key ID of MN-FA key.
Parent TLV(s)	MIP4 Security Info

5.3.2.100 MS Authorization Context

Type	100	
Length in octets	Variable	
Value	Compound	
Description		
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	MS NAI	M
	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[1]
	Visited Authorized Network Services	O
	Certified-MS-Feature-List-For-GW	O[2]
	Certified-MS-Feature-List-For-BS	O[3]
	PA_VC (MSKHash1)	O
	CMAC_KEY_COUNT (PA_NONCE)	O
	NA_NONCE (Nonce2)	O
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.

5.3.2.101Target Care-of Address

Type	101
Length in octets	4
Value	
Description	
Parent TLV(s)	MIP4 Info

5.3.2.102 MSID

Type	102
Length in octets	6
Value	48-bit MS/AMS MAC address.
Description	Unique MS/AMS identifier (MS/AMS MAC address) (Note 1).
Parent TLV(s)	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[29]

Type	103	
Length in octets	Length of MS Info is set as 'Variable'.	
Value	Compound	
Description	Information about the MS/AMS.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	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

[29] 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.

	BS-originated EAP-Start Flag	O
	CMAC_KEY_COUNT	O
	VLAN Tag Processing Rule	O (Note 8)
	Key Change Indicator	O (Note 9)
	State	O (Note 10)
	MS MAC Version	O
	NSP ID	O
	Mobility Access Classifier	O
	Reattachment Zone	O
	LBS Loc Info	O
	LBS Transaction ID	O
	LBS Result Code	O
	NA_VC (MSKHash2)	O (Note 11)
	FQDN of new NAS Identifier	O (Note 12)
	MSID*	O(Note 13)
	STID	O(Note 14)
	CRID	O(Note 15)
	IPv4-Host-Address	O(Note 16)
	IPv6-Home-Network-Prefix	O(Note 16)
	Additional-Host-Configurations	O(Note 16)
	Basic CID	O(Note 17)
	DCR Context	M (In DCR_Entry_Req and DCR_Exit_rsp messages)
Message Primitives That Use This TLV	Every Message	

Notes

1. 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.

2. 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.

3. 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/ABS) 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/AMS.

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.

4. 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.

5. MS Security History is mandatory when MS Info is included in Relocation_Notify message.

6. MS Authorization Context is mandatory when MS Info is included in Relocation_Notify_Rsp and Relocation_Req messages.

7. Authentication Result is mandatory when MS Info is included in Relocation_Complete message.

8. If used for prepaid accounting, present with PPAQ to continue prepaid accounting session.

9. Key Change Indicator is mandatory when MS Info is included in Key_Change_Cnf message or MS_Attachment_Req message.

10. VLANTagProcessingRule exists only for ETH-CS

11. NA_VC (MSKHash2) is mandatory when authenticator shifting is used.

12. FQDN of new NAS Identifier (i.e. the new authenticator ID).

13. MSID* is mandatory when MSID privacy is enabled in Rel.2.0 operation.

14. STID, which ABS assigns uniquely to AMS, is mandatory in case of Rel.2.0 operation.

15. CRID is assigned to the AMS is in DCR mode entry of Rel.2.0 operation.

16. If Fast IP address allocation is applied, IPv4-Host-Address/ IPv6-Home-Network-Prefix/ Additional-Host-Configurations

17. In case of uncontrolled handover from the LZone of an ABS to the MZone, Basic CID indicates the AMS in combination with the serving BSID.

1 5.3.2.104 MS Mobility Mode

Type	104
Length in octets	2 byte
Value	Enumerator. The values are: • 0x0000 = PMIP4 • 0x0001 = CMIP4 • 0x0002 = CMIP6 • 0x0003 = PMIP6 • 0x0004 = MIP based ETH All other values are Reserved.
Description	Indicates which R3 mobility the MS/AMS is using.
Parent TLV(s)	Anchor MM Context

2 5.3.2.105 MS NAI

Type	105
Length in octets	Variable up to 256 octets
Value	ASCII String.
Description	MS Network Access Identifier character string.
Parent TLV(s)	MS Security History, MIP4 Security Info, MS Authorization Context

3 5.3.2.106 MS MAC Version

Type	106
Length in octets	1
Value	1 Byte value
Description	Indicates MS MAC Version per IEEE 802.16 standard. The MAC Version Value is, indicated in TLV-148 during Network entry.
Parent TLV(s)	MS Info

5.3.2.107 Void

5.3.2.108 MS Security History

Type	108	
Length in octets	Variable	
Value	Compound TLV	
Description	Security parameters presenting the history of MS authentication.	
Elements (Bus-TLVs)	**TLV Name**	**M/O**
	PMK SN	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]
Parent TLV(s)	MS Info	

Note 1: Authorization policy support TLV in MS Security History indicates the authentication modes as previously negotiated with MS/AMS. in Authenticator Relocation procedure.

Note 2: If MS/AMS 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

Type	109
Length in octets	1
Value	Enumerator. The values are: • 0x00 = MS Power Down indication (used if Network Exit Indicator is requested in RNG-REQ/AAI-RNG-REQ). • 0x01 = Radio link with MS/AMS is lost. All other values are Reserved.
Description	Present in operations related to MS Network Exit and indicates MS Network Exit reason.
Parent TLV(s)	Path Control messages (*Path_Dereg_Req*), MS State Change messages.

5.3.2.110 Newer TEK Parameters

Type	110	
Length in octets	Variable	
Value	Compound TLV	
Description	Set of the Newer TEK Parameters.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	TEK	M
	TEK SN	M
	TEK Lifetime	M
	PN Counter	O
	RxPN Counter	O
Parent TLVs	SA Descriptor	

5.3.2.111 NRT-VR Data Delivery Service

Type	111	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains the QoS parameters relevant for NRT-VR Data Delivery Service. If included in QoS Parameters, it implies nrtPS Scheduling Service for UL connections.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Minimum Reserved Traffic Rate	M
	Traffic Priority	O (if omitted means Traffic Priority = 0)
	Maximum Sustained Traffic Rate	O (if absent defaulting to Minimum Reserved Traffic Rate)
	Request/Transmission Policy	O (see Note [a])
	Maximum Traffic Burst	O
Parent TLV	QoS Parameters	

Note [a]: Used during Service flow creation, HO/ Idle Mode entry/exit operations.

5.3.2.112 Older TEK Parameters

Type	112	
Length in octets	Variable	
Value	Compound TLV	
Description	Set of the Older TEK Parameters.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	TEK	M
	TEK SN	M
	TEK Lifetime	M
	PN Counter	O
	RxPN Counter	O
Parent TLVs	SA Descriptor	

5.3.2.113 Old Anchor PC ID

Type	113
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets)
Value	Unique identifier for the Old Anchor Paging Controller network entity, which administers paging activity for the MS while in Idle Mode and retains MS service and operational information. The Identifier might be in format of either 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.
Description	
Parent TLV(s)	Paging Information

5.3.2.114 Packet Classification Rule / Media Flow Description (one or more)

Type	114	
Length in octets	Variable	
Value	Compound	
Description	Contains sub-elements representing 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.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Classification Rule Index	O
	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[1]
	MAC Destination Address and Mask	O[1]
	ETYPE/SAP	O[1]
	User Priority Range	O[1]
	SVLAN ID	O[1,2]
	CVLAN ID	O[1,3]
	IPv6 Flow Label	O
Parent TLV	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 ID is only used in downlink classification in ASN.

3 Note 3: The CVLAN ID is used as VLAN ID in uplink.

4 ### 5.3.2.115 Paging Announce Timer

Type	115
Length in octets	2 octet
Value	16-bit unsigned integer (in seconds).
Description	The duration which the MS should be paged. Paging Announce timer = 0xFFFF means that a PagingAgent SHALL apply its internal timer value and/or algorithm. The PagingAgent will continue paging the MS/AMS until it receives a Paging::Stop message for the MS/AMS, or the internal timer value expires, or an implementation-specific algorithm decides to stop the paging – whichever comes first. PagingAnnounce timer = 0 stands for a single page. PagingAnnounce timer > 0 implies that the Paging Agent will page the MS/AMS until this timer value (in seconds) expires. If PagingAnnounce timer is omitted, then a value of 0 is assumed.
Parent TLV(s)	Paging Information

5.3.2.116 Paging Cause

Type	116
Length in octets	1
Value	Enumerator. The values are: • 0x01 = Location update. • 0x02 = Network Re-Entry, Incoming Data for Idle MS/AMS. All other values are Reserved.
Description	
Parent TLV(s)	Paging Information

5.3.2.117 Relay PC ID

Type	117
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets).
Value	Unique identifier for the Paging Controller network entity, which takes part in forwarding of Idle mode and Paging related network messages between the MS/AMS 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/AMS's Anchor PC is not in serving ASN. The Identifier has same format as Anchor PC ID.
Description	
Parent TLV(s)	Paging Information

5.3.2.118 Paging Cycle

Type	118
Length in octets	2
Value	
Description	Cycle in which the paging message is transmitted within the paging group (aligned with 802.16e/m).
Parent TLV(s)	Paging Information

1 ### 5.3.2.119 Paging Information

Type	119	
Length in octets	Variable	
Value	Compound TLV	
Description	Set of Paging related IEs.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Paging Cycle	O
	Paging Offset	O
	Paging Interval Length	O
	Relocation Success Indicator	O
	Paging Group ID	O
	Deregistration ID	O
	current Paging Cycle	O
	current Paging Offset	O
	current Deregistration ID	O
	current 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
Message Primitives That Use This TLV	Paging Function messages; Data Path Control messages; Context Delivery messages.	

5.3.2.120 Paging Offset

Type	120
Length in octets	2
Value	
Description	Determines the frame within the cycle in which the paging message is transmitted. SHALL be smaller than the PAGING CYCLE value.
Parent TLV(s)	Paging Information

5.3.2.121 Paging Start/Stop

Type	121
Length in octets	1
Value	
Description	Indicates to the BS/ABSs whether to start/stop paging on the airlink.
Parent TLV(s)	Paging Information

5.3.2.122 PC Relocation Indication

Type	122
Length in octets	1
Value	
Description	Request from the Current Anchor PC to the New Anchor PC to perform PC relocation.
Message Primitives That Use This TLV	R4 *LU_Rsp*

5.3.2.123 Paging Group ID

Type	123
Length in octets	2
Value	Byte string
Description	16-bit ID representing Paging Group.
Parent TLV(s)	Paging Information

5.3.2.124 PHSF

Type	124
Length in octets	Variable
Value	Byte string
Description	String of bytes containing the header information to be suppressed.
Parent TLV	PHS Rule

1 5.3.2.125 PHSI

Type	125
Length in octets	1
Value	8-bit unsigned integer.
Description	PHSI has a value between 1 and 255, which uniquely references the suppressed byte string. The index is unique per service flow. The uplink and downlink PHSI values are independent of each other.
Parent TLV	PHS Rule

2 5.3.2.126 PHSM

Type	126
Length in octets	Variable
Value	Bit string
Description	The value of this field is used to interpret the values in the PHSF. It is used at both the sending and receiving entities. The PHSM allows fields, such as sequence numbers or checksums (which vary in value), to be excluded from suppression with the constant bytes around them suppressed: • Bit #0: 0 = Do not suppress first byte of the suppression field, 1 = Suppress first byte of the suppression field. • Bit #1: 0 = Do not suppress second byte of the suppression field, 1 = Suppress second byte of the suppression field. • Bit #x: 0 = Do not suppress (x+1) byte of the suppression field, 1 = Suppress (x+1) byte of the suppression field.
Parent TLV	PHS Rule

3 5.3.2.127 PHS Rule

Type	127	
Length in octets	Variable	
Value	Compound	
Description	Parameters associated with a PHS Rule. Omission means PHS is disabled.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	PHSI	O
	PHSS	O
	PHSF	O
	PHSM	O
	PHSV	O
	PHS Rule Action	O
Parent TLV	SF Info	

5.3.2.128 PHS Rule Action

Type	128
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Add PHS Rule • 0x01 = Set PHS Rule • 0x02 = Delete PHS Rule • 0x03 = Delete All PHS Rules All other values are Reserved.
Description	PHS Action Code. The Set PHS Rule command is used to add the specific TLVs for an undefined PHS rule. It shall NOT be used to modify existing TLVs. When deleting all PHS Rules, any corresponding PHSI shall be ignored. An attempt to add a PHS Rule that already exists is an error condition.
Parent TLV	PHS Rule

5.3.2.129 PHSS

Type	129
Length in octets	1
Value	8-bit unsigned integer.
Description	The value of this field is the total number of bytes in the header to be suppressed and then restored in a service flow that uses PHS. This TLV is used when a service flow is being created. For all packets that get classified and assigned to a service flow with PHS enabled, suppression SHALL be performed over the specified number of bytes as indicated by the PHSS and according to the PHSM. If this TLV is not included in a service flow definition, or is included with a value of 0 bytes, then PHS is disabled. A nonzero value indicates PHS is enabled.
Parent TLV	PHS Rule

5.3.2.130 PHSV

Type	130
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Verify • 0x01 = Don't verify All other values are Reserved.
Description	The value of this field indicates to the sending entity whether or not the packet header contents are to be verified prior to performing suppression. If PHSV is enabled, the sender SHALL compare the bytes in the packet header with the bytes in the PHSF that are to be suppressed as indicated by the PHSM.
Parent TLV	PHS Rule

5.3.2.131 PPAQ

Type	131	
Length in octets	Variable	
Value	Compound	
Description	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. 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).	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	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[30]
Parent TLV	MS Info	

[30] SF ID(s) shall be included in flow based prepaid accounting scenario.

5.3.2.132 Duration Used

Type	132
Length in octets	4
Value	Unsigned Integer representing seconds.
Description	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.
Parent TLV(s)	PPAQ

5.3.2.133 PMK SN

Type	133
Length in octets	1
Value	0X0000 | 4-bit PMK SN.
Description	PMK Sequence Number as specified by IEEE 802.16e.
Parent TLV(s)	MS Security History

5.3.2.134 PKMv2/v3 Message Code

Type	134
Length in octets	1
Value	Enumerator. The values are: • 0x0x12 = EAP Transfer All other values are Reserved.
Description	The value of this parameter indicates to BS the message code that SHOULD be used on PKMv2/v3 and indirectly the state of authentication process.
Parent TLV(s)	Authentication Complete

5.3.2.135 Paging Interval Length

Type	135
Length in octets	2
Value	Unsigned 32-bit integer
Description	Max duration in frames of Paging Listening interval. Used in calculation of Paging listening interval (aligned with 802.16).
Parent TLV(s)	Paging Information

1 5.3.2.136 PN Counter

Type	136
Length in octets	4
Value	Unsigned 32-bit integer.
Description	Last value of PN Counter used on DL (for AES CCM cipher suite). In case that PKMv3 is applied, size of PN is defined as 22bits so that 10 MSBs of PN Counter are filled with zeros.
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

2 5.3.2.137 Preamble Index / Sub-channel Index

Type	137
Length in octets	1
Value	Unsigned 8-bit integer.
Description	Represents Preamble Index/Sub-channel Index.
Parent TLV	BS Info, RRM BS Info

3 5.3.2.138 Protocol

Type	138
Length in octets	1
Value	8 bit integer, representing IP Protocol: protocol.
Description	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.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.139 Protocol Destination Port Range

Type	139
Length in octets	4
Value	This field is coded as follows: • Octet 1 = MSB of DstPortLow • Octet 2 = LSB of DstPortLow • Octet 3 = MSB of DstPortHigh • Octet 4 = LSB of DstPortHigh
Description	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.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.140 Protocol Source Port Range

Type	140
Length in octets	4
Value	This field is coded as follows: • Octet 1 = MSB of SrcPortLow • Octet 2 = LSB of SrcPortLow • Octet 3 = MSB of SrcPortHigh • Octet 4 = LSB of SrcPortHigh
Description	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.
Parent TLV	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**
	Priority Indication	CM[2]
	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[1]
	Data Integrity	O[1]
	DSCP	O
Parent TLV	SF Info	

If no Data Delivery Service Sub-TLV is included then the service profile must be referenced by either Global Service Class Name or by Service Class Name TLVs.

Notes:

1. TLV is not applicable to MCBCS Service.
2. Priority Indication is added for ETS support

5.3.2.142 Radio Resource Fluctuation

Type	142
Length in octets	1
Value	8-bit unsigned integer.
Description	Radio Resource Fluctuation is used to indicate the degree of fluctuation in DL and UL channel data traffic throughputs. When Radio Resource Fluctuation is set to 0, it implies that the DL and UL data traffic is constant in data throughput. Hence, there is no fluctuation in Available Radio Resource. When Radio Resource Fluctuation is set to maximum value 255, the data traffic is very volatile in nature which makes the Available Radio Resource unpredictable. The Radio Resource Fluctuation for all traffic models should be in the range of 0 to 255."
Parent TLV(s)	RRM BS Info

5.3.2.143 Void

5.3.2.144 REG Context

Type	144		
Length in octets	Variable		
Value	Compound		
Description	MS/AMS REG context parameters that has been agreed between MS/AMS and BS/ABS and delivered in REG-RSP/AAI-REG-RSP message during the initial network entry of MS/AMS.		
Elements (Sub-TLVs)	**TLV Name**	**M/O**	**Applicability**
	Number of UL Transport CIDs Support	M	1,2
	Number of DL Transport CIDs Support	M	1,2
	Classification/PHS Options and SDU Encapsulation Support	O[31]	1,2,3
	Maximum Number of Classifier	O[25]	1,2,3
	PHS Support	O[25]	1,2,3
	ARQ Support	M	1,2
	DSx Flow Control	O[25]	1,2
	MCA flow control	O[32]	1,2
	Multicast polling group CID support	O[33]	1,2
	Total Number of Provisioned Service Flows	O	1,2
	Maximum MAC Data per Frame Support	O[25]	1,2
	Packing Support	M	1,2
	MAC ertPS Support	O[25]	1,2
	Maximum Number of Bursts Transmitted Concurrently to the MS	M	1,2
	HO Supported	M	1,2
	HO Process Optimization MS Timer	M	1,2
	Mobility Features Supported	M	1,2
	Sleep Mode Recovery Time	M	1,2
	Idle Mode Timeout	O[25]	1,2
	ARQ Ack Type	O[25]	1,2
	MS HO Connections Parameters Proc Time	M	1,2
	MS HO TEK Proc Time	M	1,2

[31] This TLV may be omitted when its default value is to be used

[32] The TLV is optional, and shall be included when the parameters are included in R1 REG-REQ/RSP message.

[33] The TLV is optional, and shall be included when the parameters are included in R1 REG-REQ/RSP message.

	MAC Header and Extended Sub-Header Support	M	1,2
	System Resource Retain Timer	O	1,2
	MS Handover Retransmission Timer	O	1,2
	Handover Indication Readiness Timer	M	1,2
	BS Switching Timer	M	1,2
	Power Saving Class Capability	M	1,2
	MAXIMUM ARQ BUFFER SIZE	O	3
	MAXIMUM NON ARQ BUFFER SIZE	O	3
	Multicarrier capabilities	O	3
	Zone Switch Mode Support	O	3
	Capability for supporting A-GPS Method for LBS service	O	3
	Interference mitigation supported	O	3
	E-MBS capabilities	O	3
	Channel BW and Cyclic prefix	O	3
	frame configuration to support legacy R1.0	O	3
	Persistent Allocation support	O	3
	Group Resource Allocation support	O	3
	Co-located coexistence capability support	O	3
	HO Trigger Metric Support	O	3
	EBB Handover support	O	3
	Minimal HO Reentry Interleaving Interval	O	3
	Capability for sounding antenna switching support	O	3
	Antenna configuration for sounding antenna switching	O	3
	ROHC support	O	3
	AMS initiated aGP Service Adaptation Capability:	O	3
	CS specification for default service flow	M	3
Parent TLV(s)	MS Info		

5.3.2.145 Registration Type

Type	145
Length in octets	4
Value	Enumerator. The values are: • 0x00000000 – Initial Network Entry • 0x00000001 – Handoff • 0x00000002 – In-Service Data Path Establishment • 0x00000003 – MS Network Exit • 0x00000004 – Idle Mode Entry • 0x00000005 – Idle Mode Exit • 0x00000006 – Anchor DPF Relocation • 0x00000007 – In-Service Data Path De-Registration • 0x00000008 – In-Service Data Path Modification • 0x00000009 – DCR Exit All other values are Reserved.
Description	Indication of the process which includes data path (Pre-) Registration.
Message Primitives That Use This TLV	DP Control messages (Path (Pre-/De-) Registration/Modification Request/Response/Acknowledge), HO_Req

5.3.2.146 Relative Delay

Type	146
Length in octets	1
Value	8-bit unsigned integer.
Description	Represents the Target BS Relative Delay in milliseconds.
Parent TLV	BS Info

5.3.2.147 Registration Lifetime

Type	147
Length in octets	2
Value	Registration Lifetime as defined in RFC 3344.
Description	The remaining lifetime (measured in seconds).
Parent TLV	MIP4 Info

5.3.2.148 Quota Identifier

Type	148
Length in octets	4
Value	Octet String. The Quota Identifier value (most significant bit first).
Description	Quota Identifier.

Parent TLV(s)	PPAQ

5.3.2.149 Relocation Success Indicator

Type	149
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Accept • 0x01 = Refuse All other values are Reserved.
Description	Indicates confirmation of whether the Relocation was accepted and completed by the Relocation Destination.
Parent TLV(s)	Paging Information

5.3.2.150 Request/Transmission Policy

Type	150
Length in octets	4
Value	32-bit bitmask with the following values: • Bit #0 = Service flow SHALL not use broadcast bandwidth request opportunities. (Uplink only). • Bit #1 –Service flow SHALL NOT use multicast bandwidth request opportunities. (Uplink only). • Bit #2 = Service flow SHALL not piggyback requests with data. (Uplink only). • Bit #3 = Service flow SHALL not fragment data. • Bit #4 = Service flow SHALL not suppress payload headers (CS parameter). [Note that the following description is an excerption from [13].] 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. • Bit #5 = Service flow SHALL not pack multiple SDUs (or fragments) into single MAC PDUs. • Bit #6 = Service flow SHALL not include CRC in the MAC PDU. • Bit #7 = The service flow SHALL NOT compress payload headers using ROHC. [Note that the following description is an excerption from [13].] 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. All other bits are Reserved.
Description	The value of this parameter provides the capability to specify certain attributes for the associated service flow. These attributes include options for PDU formation, and for uplink service flows, restrictions on the types of bandwidth request options that may be used. An attribute is enabled by setting the corresponding bit position to 1.
Parent TLV	BE Data Delivery Service, ERT-VR Data Delivery Service, NRT-VR Data Delivery Service, RT-VR Data Delivery Service, UGS Data Delivery Service

5.3.2.151 Reservation Action

Type	151
Length in octets	2
Value	The Action field is a 16 bit vector with the following meaning for each bit being set to "1": • Bit 15 (0x0001) = Create service flow • Bit 14 (0x0002) = Admit service flow • Bit 13 (0x0004) = Activate service flow • Bit 12 (0x0008) = Modify service flow • Bit 11 (0x0010) = Delete service flow • Bits 0 – 10 = Undefined All other bits are Reserved.
Description	Identifies the requested resource reservation action. More than one of bits #13-#15 MAY be set to 1 at the same time (for instance, create & admit, or create/admit/activate/ modify a service flow).
Parent TLV	SF Info

5.3.2.152 Reservation Result

Type	152
Length in octets	2
Value	Result can be one of the following: • 0x0000 = Successfully Created • 0x0001 = Request Denied – No resources • 0x0002 = Request Denied due to Policy • 0x0003 = Request Denied due to Requests for Other Flows Failed • 0x0004 = Request Failed (Unspecified reason) • 0x0005 = Request Denied due to MS reason • Values in the range 0x0006 – 0xFEFF are Reserved • Values in the range 0xFF00 – 0xFFFF are Reserved
Description	Indicates the result of a Resource Reservation Request.
Parent TLV	SF Info

5.3.2.153 Response Code

Type	153
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Not allowed - Paging Reference is zero • 0x01 = Not allowed - No such SF All other values are Reserved.
Description	Indicates reason for not paging the MS/AMS.
Message Primitives that Use This TLV	Initiated_Paging_Rsp

5.3.2.154 Result Code

Type	154
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Success • 0x01 = Failure – No resources • 0x02 = Failure – Not supported • 0x03 = Partial Response • 0x04 = Multiple Not Supported • 0x05 = Request Failure • The values in the range 0x06 – 0x99 are Reserved • The values in the range 0xA0 – 0xFF are Reserved
Description	Indicates if the requested action was successfully supported at the intended target.
Message Primitives that use this TLV	HO related messages, Path (pre-)registration and context related messages.

5.3.2.155 Void

5.3.2.156 Round Trip Delay

Type	156
Length in octets	1
Value	8-bit integer representing Serving BS/ABS Round Trip Delay in the units of 1/Fs.
Description	
Parent TLV	BS Info

5.3.2.157 RRM Absolute Threshold Value J

Type	157
Length in octets	1
Value	Enumerator. The values are: • 0x00 = 0% • 0x01 = 1% • ... • 0x64 = 100% All other values are Reserved.
Description	The threshold value J is used by BS/ABS (RRA) as the absolute threshold for reporting.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

5.3.2.158 RRM Averaging Time T

Type	158
Length in octets	2
Value	16-bit unsigned integer, in units of 100 msec.
Description	Used by BS/ABS (RRA) as the measurement interval for producing the information requested by RRC.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

5.3.2.159 RRM BS Info

Type	159	
Length in octets	Variable	
Value	Compound	
Description	Contains a description of BS parameters which are not related to a specific MS/ABS.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	BS ID	M
	Available Radio Resource DL	O
	Total Slots DL	O
	Available Radio Resource UL	O
	Total Slots UL	O
	Radio Resource Fluctuation	O
	DCD/UCD Configuration Change Count	O
	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
Message Primitives That Use This TLV	RRM *Spare_Capacity_Rpt*, RRM *Neighbor_BS_Resource_Status_Update*, RRM *Radio_Config_Update_Rpt*.	

1 ### 5.3.2.160 RRM BS-MS PHY Quality Info

Type	160	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains the PHY quality indicators of the radio channel between a BS and a specific MS identified by MSID in the message header.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	BS ID	M
	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
Message Primitives That Use This TLV	RRM PHY_Parameters_Rpt	

2 ### 5.3.2.161 RRM Relative Threshold RT

Type	161
Length in octets	1
Value	Enumerator. The values are: • 0x00 = 0% • 0x01 = 1% • ... • 0x64 = 100% All other values are Reserved.
Description	The threshold value RT is used by BS/ABS (RRA) to keep track of the threshold from the last measurement period.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

5.3.2.162 RRM Reporting Characteristics

Type	162
Length in octets	4
Value	32-bit bitmask with the following values. • Bit #0 = periodically as defined by reporting period P • Bit #1 = regularly whenever resources have changed as defined by RT since the last measurement period. • Bit #2 = regularly whenever resources cross predefined total threshold(s) defined by reporting absolute threshold values J • Bit #3 = DCD/UCD Configuration Change Count modification • All Bit = 0 means “Stop RRM Reporting”, if the TLV in the Request message, and “RRM Reporting Stopped”, if the TLV is in the Report Message. All other bits are Reserved.
Description	Indicates whether reporting SHALL be once, or periodically, or event driven, in which case the event is specified.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

5.3.2.163 RRM Reporting Period P

Type	163
Length in octets	2
Value	16-bit unsigned integer, in units of 100 msec.
Description	Used by BS/ABS (RRA) as the reporting period for producing the information requested by RRC. When a report has been sent at time T, then the next report SHALL be sent at T + P, unless an earlier report is sent because of a different reporting event during that period. Whenever a report has been sent for any other reason, the timer for periodic reporting SHALL be reset at the reporting side.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

5.3.2.164 RRM Spare Capacity Report Type

Type	164
Length in octets	1
Value	Enumerator. The values are: • 0x00 = “Type 1” which refers to reporting of the “Available radio resource indicator” All other values are Reserved.
Description	The value of this parameter specifies the type of RRM *Spare_Capacity_Rpt* Forward compatibility.
Message Primitives That Use This TLV	RRM *Spare_Capacity_Req*, RRM *Spare_Capacity_Rpt*.

5.3.2.165 RT-VR Data Delivery Service

Type	165	
Length in octets	Variable	
Value	Compound	
Description	This compound TLV contains the QoS parameters relevant for RT-VR Data Delivery Service. If included in QoS Parameters, it implies rtPS Scheduling Service for UL connections.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Minimum Reserved Traffic Rate	M
	Maximum Latency	M
	Unsolicited Polling Interval	O
	Traffic Priority	O (if omitted means Traffic Priority = 0)
	Maximum Sustained Traffic Rate	O (if absent defaulting to Minimum Reserved Traffic Rate)
	Request/Transmission Policy	O (see Note [a])
	Maximum Traffic Burst	O
Parent TLV	QoS Parameters	

Note [a]: Used during Service flow creation, HO/ Idle Mode entry/exit operations.

5.3.2.166 RxPN Counter

Type	166
Length in octets	4
Value	Unsigned 32-bit integer.
Description	Last value of PN Counter used on UL (for AES CCM cipher suite). In case that PKMv3 is applied, size of PN is defined as 22bits so that 10 MSBs of PN Counter are filled with zeros.
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

5.3.2.167 Volume Quota

Type	167
Length in octets	4
Value	The attribute is an unsigned Integer representing a volume measured in kilo-bytes (1024 bytes).
Description	Indicates the volume (in octets) allocated for the session or the total used volume (in octets) for both inbound and outbound traffic.
Parent TLV(s)	PPAQ

5.3.2.168 Volume Threshold

Type	168
Length in octets	4
Value	The attribute is an unsigned Integer representing a volume measured in kilo-bytes (1024 bytes).
Description	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.
Parent TLV(s)	PPAQ

5.3.2.169 SAID

Type	169
Length in octets	2
Value	SAID definition as per 802.16.
Description	The SAID is a 16-bit identifier for the SA.
Parent TLV(s)	SF Info, SA Descriptor

5.3.2.170 SA Descriptor

Type	170	
Length in octets	Variable	
Value	Compound TLV	
Description	Set of SA-related IEs.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	SAID	M
	SA Type	M
	SA Service Type	O
	Cryptographic Suite	M
	Older TEK Parameters	O
	Newer TEK Parameters	O
Parent TLVs	MS Info	

5.3.2.171 Certified-MS-Feature-List

Type	171	
Length in octets	Variable	
Value	Compound TLV	
Description	List of CVS feature packages for the MS/AMS that are relevant for the ASN policy for this MS/AMS. The ASN-GW will populate this TLV with the information received by the AAA server across R3 in the Certified-MS-Feature-List Attribute/AVP. The ASN-GW will forward the information to the BS/ABS across R4/R6, or to another ASN-GW across R4. The TLV MUST contain one Feature-Package-List-Version TLV followed by one Feature-Package-List TLV where the feature package numbers defined by Table A-1 (ASN feature packages) in “Annex A: “ MUST be used. The ASN-GW MUST not include more than one instance of this attribute with an identical Feature-Package-List-Version value. If an ASN-GW or BS/ABS receive this TLV with an unknown Feature-Package-List-Version, it SHALL ignore this compound TLV. This document does not define any specific behavior upon receipt of the certified MS/AMS feature list and assumes this to be internal to the BS/ABS and/or ASN-GW.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Feature-Package-List-Version	M
	Feature-Package-List	M
Parent TLVs	MS Authorization Context	

5.3.2.172 SA Service Type

Type	172
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Unicast Service • 0x01 = Group Multicast Service • 0x02 = MBS Service All other values are Reserved.
Description	This attribute indicates service types of the corresponding SA type. This attribute SHALL be included only when the SA type is Static SA or Dynamic SA. The GTEK SHALL be used to encrypt connection for group multicast service.
Parent TLV(s)	SA Descriptor

5.3.2.173 SA Type

Type	173
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Primary • 0x01 = Static • 0x02 = Dynamic All values in the range 0x80 – 0xFF are Vendor Specific. All other values are Reserved.
Description	Type of SA.
Parent TLV(s)	SA Descriptor

5.3.2.174 SBC Context

Type	174		
Length in octets	Variable		
Value	Compound		
Description	MS/AMS SBC context parameters that has been agreed between MS/AMS and BS/ABS and delivered in SBC-RSP/AAI-SBC-RSP message during the initial network entry of MS/AMS.		
Elements	**TLV Name**	**M/O**	**Appliability**
	Subscriber Transition Gaps	M	1,2
	Maximum Transmit Power	M	1,2,3
	Capabilities for Construction and Transmission of MAC PDUs	M	1,2
	PKM Flow Control	O[25]	1,2
	Maximum Number of Supported Security Associations	O[25]	1,2
	Security Negotiation Parameters	M	1,2,3

	Association type support	O	1,2
	Extended Subheader Capability	M	1,2
	HO Trigger Metric Support	M	1,2
	Current Transmit Power	M	1,2
	OFDMA SS FFT Sizes	M	1,2,3
	OFDMA SS demodulator	M	1,2
	OFDMA SS modulator	M	1,2
	The number of UL HARQ Channel	M	1,2
	OFDMA SS Permutation support	M	1,2
	OFDMA SS CINR Measurement Capability	M	1,2
	The number of DL HARQ Channels	M	1,2
	HARQ Chase Combining and CC-IR Buffer Capability	M	1,2
	OFDMA SS Uplink Power Control Support	M	1,2
	OFDMA SS Uplink Power Control Scheme Switching Delay	M	1,2
	OFDMA MAP Capability	M	1,2
	Uplink Control Channel Support	M	1,2
	OFDMA MS CSIT Capability	M	1,2
	Maximum Number of Burst per Frame Capability in HARQ	O[25]	1,2
	OFDMA SS demodulator for MIMO Support	M	1,2
	OFDMA SS modulator for MIMO Support	M	1,2
	OFDMA multiple DL burst profile capability	O	1,2
	SDMA Pilot capability	O	1,2
	OFDMA Parameters Sets	O[34]	1,2
	HARQ Context	O	1,2
	CAPABILITY_INDEX	O	3
	DEVICE_CLASS	O	3
	CLC Request	O	3
	Long TTI for DL	O	3
	UL sounding	O	3
	OL Region	O	3
	DL resource metric for FFR	O	3

[34] All TLVs must be present except if the "OFDMA parameters sets" TLV is present.

	Max. Number of streams for SU-MIMO in DL MIMO	O	3
	Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	O	3
	DL MIMO mode	O	3
	feedback support for DL	O	3
	Subband assignment A-MAP IE support	O	3
	DL pilot pattern for MU MIMO	O	3
	Number of Tx antenna of AMS	O	3
	Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	O	3
	Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	O	3
	UL pilot pattern for MU MIMO	O	3
	UL MIMO mode	O	3
	Modulation scheme	O	3
	UL HARQ buffering capability	O	3
	DL HARQ buffering capability	O	3
	AMS DL processing capability per sub-frame	O	3
	AMS UL processing capability per sub-frame	O	3
	FFT size(2048/1024/512)	O	3
	Inter-RAT Operation Mode	O	3
	Supported Inter-RAT type	O	3
	MIH Capability Supported	O	3
Parent TLV(s)	MS Info		

5.3.2.175 SDU BSN Map

Type	175
Length in octets	Variable
Value	Bitmap expressing which Blocks of the SDU have been transmitted and/or acknowledged.
Description	
Parent TLV	SDU Info

5.3.2.176 SDU Info

Type	176	
Length in octets	Variable	
Value		
Description	Information about an SDU involved in Data Path Integrity operations.	
Elements (Sub-	**TLV Name**	**M/O**

TLVs)	SDU SN	M
	SDU BSN Map	O
	Pointer BSN	O
Parent TLV	SF Info	

1 5.3.2.177 SDU Size

Type	177
Length in octets	1
Value	8-bit unsigned integer. Default = 49.
Description	Represents the number of bytes in the fixed size SDU. This parameter may be used for a UGS service flow when the length of IP packets on the data plane is fixed and known in advance (this is typically the case for flows generated by a specific codec).
Parent TLV	UGS Data Delivery Service

2 5.3.2.178 SDU SN

Type	178
Length in octets	4
Value	SDU Sequence Number (for Data Path Integrity operations).
Description	
Parent TLV	SDU Info

3 5.3.2.179 Service Class Name

Type	179
Length in octets	2 – 128
Value	Service Class Name as defined in IEEE802.16e/m.
Description	ASCII string, which is known at the BS/ABS and which indirectly specifies a set of QoS Parameters.
Parent TLV	QoS Parameters R3 QoS Descriptor

4 5.3.2.180 Service Level Prediction

Type	180
Length in octets	1
Value	8-bit integer representing Service Level Prediction.
Description	
Parent TLV	BS Info

1 5.3.2.181 Service Authorization Code

Type	181
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Service authorized • 0x01 = Service not authorized All other values are Reserved.
Description	Code indicating whether or not service is authorized.
Parent TLV	MS Info

2 5.3.2.182 Serving/Target Indicator

Type	182
Length in octets	1
Value	Enumerator: The values are: • 0x00 = Serving • 0x01 = Target All other values are Reserved.
Description	Indicates if the designated BS is the Serving BS/ABS or Target BS/ABS for the handover.
Message Primitives That Use This TLV	HO related messages.
Parent TLV(s)	BS Info, RRM BS_MS PHY Quality Info

3 5.3.2.183 Feature-Package-List-Version

Type	183
Length in octets	2
Value	The value is set to ‘1’. All other values are reserved for future use.
Description	The version of the subsequent Feature-Package-List.
Parent TLV(s)	Certified-MS-Feature-List

4 5.3.2.184 SFID

Type	184
Length in octets	4
Value	32-bit unsigned integer.
Description	SFID definition as per 802.16.
Parent TLV(s)	SF Info

5.3.2.185 SF Info

Type	185	
Length in octets	Variable	
Value	Compound	
Description	Service Flow Description.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Failure Indication Details	O[1]
	SFID	O
	SF Type	O
	Reservation Action	O[1]
	Reservation Result	O[1]
	HARQ Context	O
	ARQ Enable	O[1]
	ARQ Context	O[1]
	ARQ Window Info	O[1]
	SN Feedback Enabled field	O
	FSN Size	O
	Direction	O[1]
	CID/MCID	O[2]
	FID	O
	SAID	O[1]
	Packet Classification Rule / Media Flow Description (one or more)	O
	QoS Parameters	O
	VLANTagProcessingRuleID	O
	Paging Preference	O[1]
	CS Type	O
	Data Integrity Method	O
	Data Path Info	O
	SDU Info	O[1]
	PHS Rule	O[1]
	Accounting Extension	O
	SA Descriptor	O[1]
	Correlation ID	O
	Data Delivery Trigger	O
	Pointer BSN	O

	BSN ARQ State Bitmap	$O^{1, 5}$
	MCBCS Service continuity indicator	O^{3}
	MBS Zone ID	O^{3}
	MCBCS Transmission Zone ID	$O^{3,4}$
	PDFID	$O^{3,4}$
	Data Integrity Applied	O
	SF Operation Policy	O
	Local Routing Policy	O
Parent TLV(s)	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. This TLV is not included if there are no ARQ blocks to be forwarded or if ARQ is disabled for the service flow.

5.3.2.186 Spare Capacity Indicator

Type	186
Length in octets	2
Value	16-bit signed integer.
Description	The value defines how many MS/AMSs with certain Quality Of Service Parameters and certain PHY Quality Info may be accommodated. Negative value indicates that even the existing MS/AMSs suffer from degradation of service.
Parent TLV	BS Info

5.3.2.187 TEK

Type	187
Length in octets	Two fixed sizes, either 8 or 16
Value	64-bit or 128-bit string.
Description	Traffic Encryption Key.
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

1 5.3.2.188 TEK Lifetime

Type	188
Length in octets	4
Value	32-bit unsigned integer.
Description	The remaining TEK Lifetime in seconds. The value 0x00000000 means that the corresponding TEK is not valid.
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

2 5.3.2.189 TEK SN

Type	189
Length in octets	1
Value	Enumerator. The values are: • 0x00 = TEK Sequence Number 0 • 0x01 = TEK Sequence Number 1 • 0x02 = TEK Sequence Number 2 • 0x03 = TEK Sequence Number 3 All other values are Reserved.
Description	2-bit TEK Sequence Number.
Parent TLV(s)	Older TEK Parameters, Newer TEK Parameters

3 5.3.2.190 Tolerated Jitter

Type	190
Length in octets	4
Value	32-bit unsigned integer (in milliseconds).
Description	This parameter represents the maximum delay variation (jitter) (in milliseconds).
Parent TLV	• UGS Data Delivery Service • ERT-VR Data Delivery Service • R3 QoS Descriptor

4 5.3.2.191 Total Slots DL

Type	191
Length in octets	2
Value	16-bit unsigned integer.
Description	Total number of slots in the DL frame. This is the total (max) number of slots possible in DL. This would depend on the RF channelization and the subchannelization schemes employed.
Parent TLV(s)	RRM BS Info

1 5.3.2.192 Total Slots UL

Type	192
Length in octets	2
Value	16-bit unsigned integer.
Description	Total number of slots in the UL frame. This is the total (max) number of slots possible in UL. This would depend on the RF channelization and the subchannelization schemes employed.
Parent TLV(s)	RRM BS Info

2 5.3.2.193 Traffic Priority

Type	193
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Priority 0 • 0x01 = Priority 1 • 0x02 = Priority 2 • 0x03 = Priority 3 • 0x04 = Priority 4 • 0x05 = Priority 5 • 0x06 = Priority 6 • 0x07 = Priority 7 All other values are Reserved.
Description	The value of this parameter specifies the priority assigned to a service flow as it is defined for the Traffic Priority in IEEE802.16e [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.
Parent TLV	• BE Data Delivery Service • UGS Data Delivery Service • NRT-VR Data Delivery Service • RT-VR Data Delivery Service • ERT-VR Data Delivery Service • R3 QoS Descriptor

5.3.2.194 Tunnel Endpoint

Type	194
Length in octets	Variable (either 4 or 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	Specifies the IP Address of the GRE tunnel associated with the Data Path. If omitted than the IP Address is defaulted to the Source Address of the sender of Path (Pre-) Registration Request.
Parent TLV(s)	Data Path Info

5.3.2.195 UCD Setting

Type	195
Length in octets	Variable
Value	Compound, as specified in [802.16e-2005], section 11.1.7.
Description	This is an IEEE802.16e-2005 defined TLV. The UCD_settings is a TLV value that encapsulates a UCD message (excluding the generic MAC header and CRC) that may be transmitted in the advertised BS downlink channel. This information is intended to enable fast synchronization of the MS with the advertised BS downlink. The UCD settings fields SHALL contain only neighbor’s UCD TLV values that are different from the serving BS corresponding values. For values that are not included, the MS SHALL assume they are identical to the corresponding values of the serving BS. The duplicate TLV encoding parameters within a Neighbor BS SHALL not be included in UCD setting. See [802.16e-2005], section 11.1.7.
Parent TLV(s)	RRM BS Info

5.3.2.196 UGS Data Delivery Service

<table>
<tr><td><b>Type</b></td><td colspan="2">196</td></tr>
<tr><td><b>Length in octets</b></td><td colspan="2">Variable</td></tr>
<tr><td><b>Value</b></td><td colspan="2">Compound</td></tr>
<tr><td><b>Description</b></td><td colspan="2">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.</td></tr>
<tr><td rowspan="6"><b>Elements (Sub-TLVs)</b></td><td><b>TLV Name</b></td><td><b>M/O Flag</b></td></tr>
<tr><td>Minimum Reserved Traffic Rate</td><td>O (when included it is set to same value as Maximum Sustained Traffic Rate)</td></tr>
<tr><td>Maximum Sustained Traffic Rate</td><td>M</td></tr>
<tr><td>Maximum Latency</td><td>M</td></tr>
<tr><td>Tolerated Jitter</td><td>O (omission means jitter equal to maximum latency)</td></tr>
<tr><td>SDU Size</td><td>O (omission means variable size SDU)</td></tr>
</table>

	Unsolicited Grant Interval	O
	Traffic Priority	O (if omitted means Traffic Priority = 0)
	Request/Transmission Policy	O (see Note [a])
Parent TLV	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

Type	197
Length in octets	4
Value	• Octet 1: 8-bit UL RSSI Mean • Octet 2: 8-bit UL RSSI Std • Octet 3: 8-bit UL CINR Mean • Octet 4: 8-bit UL CINR Std
Description	
Parent TLV	BS Info

3 5.3.2.198 UL PHY Service Level

Type	198
Length in octets	4
Value	32-bit integer representing UL PSL.
Description	
Parent TLV	BS Info

4 5.3.2.199 Unsolicited Grant Interval

Type	199
Length in octets	2
Value	16-bit unsigned integer representing the grant interval (in milliseconds).
Description	The value of this parameter specifies the nominal interval between successive data grant opportunities for this service flow. This parameter may be used for a UGS and ERT-VR service flow when the inter-arrival time of IP packets on the data plane is known in advance (this is typically the case for flows generated by a specific codec).
Parent TLV	• ERT-VR Data Delivery Service • UGS Data Delivery Service • R3 QoS Descriptor

1 ### 5.3.2.200 Unsolicited Polling Interval

Type	200
Length in octets	2
Value	16-bit unsigned integer representing the polling interval (in milliseconds).
Description	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
Parent TLV	RT-VR Data Delivery Service

2

3 ### 5.3.2.201 VAAA IP Address

Type	201
Length in octets	Variable (either 4 or 16)
Value	The length defines the format of this value – IPv4 or IPv6. The value with length of 4 octets provides IPv4 address. The value with 16 octets provides IPv6 address.
Description	VAAA IPv4 or IPv6 address.
Parent TLV(s)	MS Security History

4 ### 5.3.2.202 VAAA Realm

Type	202
Length in octets	Variable up to 256 octets
Value	ASCII String
Description	VAAA realm character string.
Parent TLV(s)	MS Security History

5 ### 5.3.2.203 BS HO RSP Code

Type	203
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Void • 0x01 = Target BS/ABS doesn’t support this HO Type • 0x02 = Target BS/ABS’s air link resource is not enough • 0x03 = Target BS/ABS’s CPU overload • 0x04 = Target BS/ABS rejects for other reasons All other values are Reserved.
Description	This TLV is used to carry HO failure reason for target BS/ABS.
Parent TLV(s)	BS Info

5.3.2.204 Accounting Context

Type	204	
Length in octets	Variable	
Value	Compound	
Description	Accounting Context.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Accounting Mode Provisioning	M
	R3 Acct Session Time	O[1]
	R3 Active Time	O[1]
	Interim Update Interval Remaining	O[2]
Message Primitives That Use This TLV	RR_Req (Create) / HO_Req/Context_Rpt / Relocation_Complete_Rsp/Anchor_DPF_HO_Req Anchor_DPF_HO_Trigger	

[1] These sub-TLVs are only included in the Relocation_Complete_Rsp message

[2] This sub-TLV is only included in the Anchor_DPF_HO_Req message

5.3.2.205 HO ID

Type	205
Length in octets	Shall follow 802.16e
Value	
Description	This IE is defined in the IEEE 802.16e spec.
Parent TLV(s)	BS Info

5.3.2.206 Combined Resource Indicator

Type	206
Length in octets	3
Value	Compound

Description	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. 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. 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. 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. Separate QoS resource reservation messages may be sent for each group of service flows indicated by the combined resource indicator.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	CS Type	M
	Combined Resources Required	M
Parent TLV(s)	MS Info	

1 ### 5.3.2.207 R3 WiMAX® Capability

Type	207	
Length	Variable	
Value	Compound	
Description		
Elements	**TLV Name**	**M/O**
	R3 WiMAX-Release	M
	R3 Accounting Capabilities	M
	R3 Hotlining Capability	M
	R3 Idle Notification Capabilities	O
Parent TLV	Ms Authorization Context	

1 5.3.2.208 R3 Accounting Capabilities

Type	208
Length	1
Value	1 octet Bit Mask with the following values: • 0x00 = No accounting. Only valid at the HA • 0x01 = Session-based accounting. Default value for the ASN • 0x02 = Flow-based accounting for IP-CS • 0x04 = Flow-based accounting for ETH-CS • The rest of the bits are reserved.
Description	Accounting Capabilities.
Parent TLV	R3 WiMAX Capability

2 5.3.2.209 R3 Idle Notification Capabilities

Type	209
Length	1
Value	Enumerator. The values are: • 0x00 = Idle Mode notification is not supported or is not required • 0x01 = Idle Mode notification is supported and is required All other values are Reserved.
Description	Idle notification Capabilities.
Parent TLV	R3 WiMAX Capability

3 5.3.2.210 R3 CUI

Type	210
Length	Variable
Value	String
Description	CUI
Parent TLV	Ms Authorization Context

4 5.3.2.211 R3 Class

Type	211
Length	Variable
Value	String
Description	Class
Parent TLV	Ms Authorization Context

5.3.2.212 R3 Framed IP Address

Type	212
Length	4
Value	32-bits unsigned integer.
Description	Framed-IP-Address.
Parent TLV	Ms Authorization Context

5.3.2.213 R3 Framed-IPv6-Prefix

Type	213
Length	Variable
Value	0-16 bytes.
Description	Framed-IPv6-Prefix.
Parent TLV	Ms Authorization Context

5.3.2.214 R3 WiMAX® Session ID

Type	214
Length	Variable
Value	String
Description	WiMAX-Session-ID.
Parent TLV	Ms Authorization Context

5.3.2.215 R3 Packet Flow Descriptor

Type	215	
Length	Variable	
Value	Compound	
Description	This TLV is used to carry Packet Flow Descriptor V2 information received over R3.	
Elements	**TLV Name**	**M/O**
	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[35]
	R3 Downlink Classifier (This TLV is deprecated in this release)	O[36]
	R3 Paging Preference	O
Parent TLV	Ms Authorization Context	

5.3.2.216 R3 Packet Data Flow ID

Type	216
Length	2
Value	Unsigned Short representing the flow identifier (most significant bit first). A value of zero(0) is invalid.
Description	Packet data flow ID.
Parent TLV	R3 Packet-Flow Descriptor

5.3.2.217 R3 Service Data Flow ID

Type	217
Length	2
Value	Unsigned Short representing the Service flow identifier (most significant bit first). This value is assigned by the home network and is unique per mobile session for the life of the session. A value of zero(0) is invalid.
Description	Service data flow ID.
Parent TLV	R3 Packet-Flow Descriptor

5.3.2.218 R3 Service Profile ID

Type	218
Length	4
Value	Unsigned Integer representing the identity of a Flow Spec that is pre-provisioned (most significant bit first). A value of zero(0) is invalid.
Description	Service Profile ID.
Parent TLV	R3 Packet-Flow Descriptor

[35] This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 only SHALL be used in this Release

[36] 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

Type	219
Length	1
Value	Enumerator. The values are: • 0x00 = Reserved • 0x01 = Uplink • 0x02 = Downlink • 0x03 = Bi-directional All other values are Reserved.
Description	Direction.
Parent TLV	R3 Packet-Flow Descriptor

2 ### 5.3.2.220 R3 Activation Trigger

Type	220
Length	1
Value	• 0x00 = Reserved • 0x01 = Provisioned (SHALL be set in case of ISF) • 0x02 = Admit (SHALL be set in case of ISF) • 0x04 = Activate (SHALL be set in case of ISF) • 0x08 = Dynamically Reservation (not valid for ISF) 0x10 to 0x80 = Reserved.
Description	Activation Trigger.
Parent TLV	R3 Packet-Flow Descriptor

3 ### 5.3.2.221 R3 Transport Type

Type	221
Length	1
Value	• 0x00 = Reserved • 0x01 = IPv4-CS • 0x02 = IPv6-CS • 0x03 = Ethernet All other values are Reserved.
Description	Transport Type.
Parent TLV	R3 Packet-Flow Descriptor

5.3.2.222 R3 Uplink QoS ID

Type	222
Length	1
Value	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.
Description	Uplink QoS ID.
Parent TLV	R3 Packet-Flow Descriptor

5.3.2.223 R3 Downlink QoS ID

Type	223
Length	1
Value	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.
Description	Downlink QoS ID.
Parent TLV	R3 Packet-Flow Descriptor

5.3.2.224 R3 Uplink Classifier (This TLV is deprecated in this release) [37]

5.3.2.225 R3 Downlink Classifier (This TLV is deprecated in this release) [38]

5.3.2.226 R3 QoS Descriptor

Type	226	
Length	Variable	
Value	Compound	
Description		
Elements	**TLV Name**	**M/O**
	R3 QoS ID	M
	Global Service Class Name	O
	Service Class Name	O
	Priority Indication	CM[1]
	R3 Schedule Type	M
	Traffic Priority	O
	Maximum Sustained Traffic Rate	O
	Minimum Reserved Traffic Rate	O

[37] This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 SHALL be used in this Release

[38] This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 SHALL be used in this Release

	Maximum Traffic Burst	O
	Tolerated Jitter	O
	R3 Maximum Latency	O
	Reduced Resources Code	O
	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
Parent TLV	Ms Authorization Context	

Notes:

1. Priority Indication is added for ETS support.

5.3.2.227 R3 QoS ID

Type	227
Length	1
Value	Unsigned Octet representing an ID.
Description	QoS ID.
Parent TLV	R3 QoS Descriptor

5.3.2.228 Media Flow Description in SDP Format

Type	228
Length in octets	Variable
Value	<SDP string> is encoded as specified in IETF RFC 2327.
Description	This is a variable length string having SDP information. The <SDP string> is encoded as specified in IETF RFC 2327.
Parent TLV	QoS Parameters

5.3.2.229 Capabilities Negotiation Mode

Type	229
Length in octets	1
Value	Indicates mode being used and is coded as follows: • 0x01 = Complete List of Capabilities • 0x02 = Partial List of Capabilities All other values are Reserved.
Description	Indicates Capability Negotiation Mode to be used
Parent TLV	Capabilities Info

5.3.2.230 R3 Schedule Type

Type	230
Length	1
Value	Enumerator. The values are: • 0x02 = Best Effort • 0x03 = nrtPS • 0x04 = rtPS • 0x05 = Extended rtPS • 0x06 = UGS All other values are Reserved.
Description	Schedule Type.
Parent TLV	R3 QoS Descriptor

5.3.2.231 Feature-Package_List

Type	263
Length in octets	Variable (2 + roundup(n/8) where n is the number of bits that corresponds to the number of feature packages)
Value	Bitmap representing the list of feature packages. The bitmap is encoded as a bitstream where bit 0 is the most significant bit which is sent first (bit 0 of the first octet). Bit 8 of the bitstream is the first bit of the second octet etc. Each bit corresponds to the feature package number as defined by "Annex A: ". A value of '0' means that the MS/AMS provided a CRN value during network entry which indicates that the MS/AMS is not certified for this feature package (or the feature package should not be enabled for this MS/AMS based on other reasons subject to the operator's policy). The number of octets depends on the number of feature packages to be encoded as identified by the respective feature package table. Example: • Bit-#0 – reserved • Bit-#1 – Feature Package 1 (0 = not certified; 1 = certified) • Bit-#2 – Feature Package 2 (0 = not certified; 1 = certified) • Etc. All bits where no feature package corresponding to the bit number is defined, are reserved. All reserved bits MUST be set to '0' by the sender and are ignored by the receiver.
Description	Indicates for each of the feature packages whether the MS is certified or not.
Parent TLV	Certified-MS-Feature-List

5.3.2.232 Optimized Relocation (OR Type)

Type	232
Length in octets	1
Value	0x00 – Idle mode OCR: Optimized Combined AA/PC/ADPF Relocation (LU-Triggered during idle mode) 0x01 - Active mode OCR: Optimized Combined AA/ADPF Relocation (active mode) 0x02 – OSR: Optimized Standalone Authenticator Relocation (regardless of active/idle mode) 0x03-0xFF- Reserved for future use.
Description	Indicate the trigger cause (including trigger condition) of Optimized Relocation
Parent TLV	MS_Info

5.3.2.233 Present Authenticator Validation Code (PA_VC)

Type	233
Length in octets	32
Value	Hash value of PA_VC (MSKHash1)
Description	
Parent TLV	MS Authorization Context

5.3.2.234 PA_NONCE

Type	234
Length in octets	2
Value	PA_NONCE (Nonce1)
Description	PA_NONCE set to CMAC_KEY_COUNT
Parent TLV	MS Authorization Context

5.3.2.235 NA_NONCE

Type	235
Length in octets	2
Value	NA_NONCE (Nonce2)
Description	
Parent TLV	MS Authorization Context

5.3.2.236 R3 Maximum Latency

Type	236
Length in octets	4
Value	32-bit integer specifies the maximum latency (in milliseconds).
Description	Time period between the reception of a packet by the BS/ABS or MS/AMS 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 /ABS or MS/AMS and SHALL be guaranteed by the BS/ABS or MS/AMS. A BS/ABS or MS/AMS does not have to meet this service commitment for service flows that exceed their minimum reserved rate.
Parent TLV	R3 QoS Descriptor

5.3.2.237 Reduced Resources Code

Type	237
Length in octets	0
Value	Value = Null, see Description.
Description	This code indicates that the requesting entity will accept reduced resources Code if the requested resources are not available.
Parent TLV	• QoS Parameters • R3 QoS Descriptor

5.3.2.238 R3 Media Flow Type

Type	238
Length in octets	1
Value	Enumerator. The values are: • 0x01 = Voice over IP • 0x02 = Robust Browser • 0x03 = Secure Browser/ VPN • 0x04 = Streaming video on demand • 0x05 = Streaming live TV • 0x06 = Music and Photo Download • 0x07 = Multi-player gaming • 0x08 = Location-based services • 0x09 = Text and Audio Books with Graphics • 0x0A = Video Conversation • 0x0B = Message • 0x0C = Control • 0x0D = Data All other values are Reserved.
Description	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
Parent TLV	R3 QoS Descriptor

5.3.2.239 New Authenticator Validation Code (NA_VC)

Type	239
Length in octets	32
Value	Hash value of NA_VC (MSKHash2)
Description	
Parent TLV	MS Info

5.3.2.240 R3 SDU Size

Type	240
Length in octets	1
Value	8-bit unsigned integer. Default = 49.
Description	Represents the number of bytes in the fixed size SDU. This parameter may be used for a UGS service flow when the length of IP packets on the data plane is fixed and known in advance (this is typically the case for flows generated by a specific codec).
Parent TLV	R3 QoS Descriptor

5.3.2.241 R3 Unsolicited Polling Interval

Type	241
Length in octets	2
Value	16-bit unsigned integer representing the polling interval (in milliseconds).
Description	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
Parent TLV	R3 QoS Descriptor

5.3.2.242 R3 Acct Interim Interval

Type	242
Length	4
Value	32-bit unsigned integer
Description	Acct-Interim-Interval.
Parent TLV	Ms Authorization Context

5.3.2.243 Accounting Mode Provisioning

In order to support the “optional” accounting agent at the BS/ABS 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.

Type	243		
Length in octets	Variable		
Value	Compound TLV		
Description	Optional accounting extensions that is designed to enable the Accounting Agent, if present, to communicate with the accounting client. The optional accounting mode provisioning TLV is included in existing messages to indicate the different accounting options as described in the stage-2 specifications.		
Elements (Sub-TLVs)	**TLV Name**	**Description**	**M/O**
	Accounting Type	The Accounting Type is 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
Parent TLV(s)	Accounting Context		

5.3.2.244 Accounting Session/Flow Volume Counts

Type	244		
Length in octets	Variable		
Value	Compound TLV		
Description	The counts represent session or flow depending on the Accounting Type that has been specified for the MS/AMS. The counts are sent by the Accounting Agent to the Accounting Client during Service Flow Deletion/Modification, HO, entering Idle Mode, entering DCR Mode, de-registering from the network, and reporting bulk interim accounting. The counts are cumulative meaning that the counts are not reset on the Accounting Agent each time the TLV is sent. Also the counts are simply the counts collected at the Accounting Agent. The overflow of any of these counters is handled by the Accounting Client.		
Elements (Sub-TLVs)	**TLV Name**	**Description**	**M/O**
	Cumulative Uplink Octets	Shall include this TLV if the value is > 0	M
	Cumulative Downlink Octets	Shall include this TLV if the value is > 0	M
	Uplink Octets at Tariff Switch		O
	Downlink Octets at Tariff Switch		O
	Cumulative Uplink Packets	Shall include this TLV if the value is > 0	M
	Cumulative Downlink Packets	Shall include this TLV if the value is > 0	M
	Uplink Packets at Tariff Switch		O
	Downlink Packets at Tariff Switch		O
Parent TLV(s)	Accounting Bulk Session/Flow		

5.3.2.245 Accounting Number of Bulk Sessions/Flows

Type	245
Length in octets	1
Value	The number of Accounting Bulk Session/Flow TLVs
Description	
Parent TLV(s)	Accounting Bulk Session/Flow Volume Counts

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		

5.3.2.247 Accounting Type

Type	247
Length in octets	1
Value	1st nibble: • 0x0 = Invalid • 0x1 = IP Session-Based Accounting Default value for the ASN • 0x2 = Flow-Based Accounting All other values are Reserved.
Description	
Parent TLV(s)	Accounting Mode Provisioning

5.3.2.248 Interim Update Interval

Type	248
Length in octets	2
Value	16-bit unsigned integer representing the interval in seconds.
Description	
Parent TLV(s)	Accounting Mode Provisioning

5.3.2.249 Cumulative Uplink Octets

Type	249
Length in octets	8
Value	Cumulative uplink volume count in octets.
Description	
Parent TLV(s)	Accounting Session/Flow Volume Counts

5.3.2.250 Cumulative Downlink Octets

Type	250
Length in octets	8
Value	Cumulative downlink volume count in octets.
Description	
Parent TLV(s)	Accounting Session/Flow Volume Counts

5.3.2.251 Cumulative Uplink Packets

Type	251
Length in octets	8
Value	Cumulative uplink volume count in packets.
Description	
Parent TLV(s)	Accounting Session/Flow Volume Counts

5.3.2.252 Cumulative Downlink Packets

Type	252
Length in octets	8
Value	Cumulative downlink volume count in packets.
Description	
Parent TLV(s)	Accounting Session/Flow Volume Counts

5.3.2.253 Time of Day Tariff Switch

<table>
<tr><td><b>Type</b></td><td colspan="2">253</td></tr>
<tr><td><b>Length in octets</b></td><td colspan="2">6</td></tr>
<tr><td><b>Value</b></td><td colspan="2">Compound TLV</td></tr>
<tr><td><b>Description</b></td><td colspan="2"></td></tr>
<tr><td rowspan="3"><b>Elements (Sub-TLVs)</b></td><td><b>TLV Name</b></td><td><b>M/O</b></td></tr>
<tr><td>1. Time of Day Tariff Switch Time</td><td>M</td></tr>
<tr><td>2. Time of Day Tariff Switch Offset</td><td>M</td></tr>
</table>

1
5.3.2.254 Time of Day Tariff Switch Time

Type	254
Length in octets	2
Value	The time of day time in hours and minutes • Octet 1: 0x00-0x17 = Hour (0-23) • Octet 2: 0x00-0x3B = Minute (0-59) All other values are Reserved.
Description	
Parent TLV(s)	Time of Day Tariff Switch

2
5.3.2.255 Time of Day Tariff Switch Offset

Type	255
Length in octets	4
Value	32-bit signed integer: Offset (+/- seconds from UTC).
Description	
Parent TLV(s)	Time of Day Tariff Switch

3
5.3.2.256 Accounting Number of ToDs

Type	256
Length in octets	1
Value	UINT8 (0 .. 255).
Description	
Parent TLV(s)	Accounting Mode Provisioning

4
5.3.2.257 Uplink Octets at Tariff Switch

Type	257
Length in octets	8
Value	Uplink octets at tariff switch.
Description	
Parent TLV(s)	Accounting Session/Flow Volume Counts

5
5.3.2.258 Downlink Octets at Tariff Switch

Type	258
Length in octets	8
Value	Downlink Octets at Tariff Switch.
Description	
Parent TLV(s)	Accounting Session/Flow Volume Counts

5.3.2.259 Uplink Packets at Tariff Switch

Type	259
Length in octets	8
Value	Uplink Packets at tariff switch.
Description	
Parent TLV(s)	Accounting Session/Flow Volume Counts

5.3.2.260 Downlink Packets at Tariff Switch

Type	260
Length in octets	8
Value	Downlink Packets at tariff switch.
Description	
Parent TLV(s)	Accounting Session/Flow Volume Counts

5.3.2.261 Vendor Specific TLV

Vendor Specific TLV is an optional TLV. When TLV type indicates Vendor Specific TLV, but the Vendor ID is not recognized, then processing SHALL silently discard the TLV and continue processing the rest of the message.

The value field of the TLV contains the Vendor Identification (Vendor ID) specified by the 24-bit vendor-specific Organization Unique Identifier (OUI) of the Network Element Vendor or Network Provider.

The content and format of the TLV is as follows:

Type	0x7FFF (524287)
Length in Octets	Variable
Value	Vendor Specific information Field (VSIF).
Description	
Message Primitives That Use This TLV	Every message

The format of the Vendor Specific Information Field (VSIF) is as follows:

- First 24 bits – Vendor ID (mandatory)
- Rest of info in TLV (optional) – vendor-specific, out of scope for standard definition

The Vendor ID field SHALL be the first field of VSIF.

Vendor Specific TLV MAY be nested inside another TLV.

Multiple Vendor Specific TLVs can be inserted into one message across R6 or R4.

Notes

Note 1: Vendor ID mentioned in this section is different from the Vendor ID specified in Section 4 and Section 5.4.2. Vendor ID in this section refers only to Organization Unique Identifier (OUI) of the Network Element Vendor or Network Provider and does not refer to Enterprise Number.

Note 2: One or more SF Info TLVs MAY be included in order to describe Service Flows in Data Path Control, Reservation, and HO Control Messages. In Data Path Control SF Info is included for Per-SF data path tunneling granularity.

Note 3: For Per-SF data path tunneling granularity, DP Info SHALL be included as sub-TLV of SF Info

Note 4: Anchor ASN GW ID points to the network entity that hosts Anchor DPF or anchor ASN GW. The content is IP address (v4 or v6).

It does not have to be included if AK Context is included. If neither Authenticator ID nor AK Context is included means that the sender of the *HO_Req* hosts the Authenticator Function for the MS/AMS.

Anchor ASN GW ID points to the network entity that hosts Anchor DPF or anchor ASN GW. The content is IP address (v4 or v6).

5.3.2.262 Paging Preference

Type	262
Length in octets	1
Value	Refer to 802.16e section 11.13.30.
Description	This parameter is a single bit indicator of an MS/AMS's preference for the reception of paging advisory messages during idle mode. When set, it indicates that the BS/ABS may present paging advisory messages or other indicative messages to the MS/AMS when data SDUs bound for the MS/AMS are present while the MS/AMS is in idle mode.
Parent TLV	SF Info

5.3.2.263 FQDN of new NAS Identifier

Type	263
Length in octets	Variable
Value	FQDN of the new NAS Identifier
Description	Indicates FQDN of the new NAS Identifier.
Parent TLV	MS Info

5.3.2.264 Accounting IP Address

Type	264
Length in octets	Variable (either 4 or 16)
Value	
Description	
Parent TLV	Accounting Bulk Session/Flow

5.3.2.265 Data Delivery Trigger

Type	265
Length in octets	1
Value	Enumerator. The values are: • 0x00 = No trigger • 0x01 = Triggers immediate delivery of data for the specified Service Flow All other values are Reserved.
Description	Triggers data delivery for the specified service flow.
Parent TLV	SF Info

5.3.2.266 MIP4 Security Info

Type	266	
Length in octets	Variable	
Value	Compound	
Description	MIP4 security context to be transferred from Anchor Authenticator to FA.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	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
Message Primitive(s) that use this TLV	Context_Rpt	

5.3.2.267 MN-FA Key Lifetime

Type	267
Length in octets	4
Value	32-bit unsigned integer.
Description	Time of MN-FA key remaining valid. This is provided to the FA by the anchor Authenticator for MN-FA key context transfer.
Parent TLV(s)	MIP4 Security Info

5.3.2.268 Idle Mode Timeout

Type	268
Length in octets	2 (as specified in 802.16e/m)
Value	16-bit unsigned integer.
Description	Maximum time interval between MS idle mode location updates in seconds, as defined in the IEEE802.16e/m.
Parent TLV(s)	Paging Information, REG Context

5.3.2.269 Classification Result

Type	269
Length in octets	1
Value	Enumerator. The values are: • 0x00 = None • 0x01 = Discard packet All other values are Reserved.
Description	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.
Parent TLV(s)	Packet Classification Rule / Media Flow Description

5.3.2.270 Network assisted HO Supported

Type	270
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Network Assisted HO not supported • 0x01 = Network Assisted HO supported All other values are Reserved.
Description	Defined in [11] Indicator for network assisted HO.
Message Primitives That Use This TLV	HO_Directive

5.3.2.271 Destination Identifier

Type	271
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets).
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	Unique identifier for the message destination.
Parent TLV	None

1 5.3.2.272 Source Identifier

Type	272
Length in octets	Variable (could be of three fixed sized: 4, 6 and 16 octets).
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 BS ID or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	Unique identifier for the message source.
Parent TLV	None

2 5.3.2.273 R3 Relocation Action

Type	273
Length in octets	1
Value	Enumerator. The values are: • 0x00 = None • 0x01 = Initiate Paging • 0x02 = Initiate FA Migration All other values are Reserved.
Description	R3 Relocation Action Code.
Message Primitives That use this TLV	Relocation_Ready_Rsp

3 5.3.2.274 Ungraceful Network Exit Indicator

Type	274
Length in octets	1
Value	Enumerator. The values are: • 0x00 – Ungraceful Network Exit No Reason • 0x01 – AAA initiated Ungraceful Network Exit • 0x02 – Authenticator initiated Ungraceful Network Exit • 0x03 – Ungraceful Network Exit by MIP session termination • 0x04 – PC initiated Ungraceful Network Exit All other values are Reserved. If a Reserved value is received then it SHALL be treated by Receiver as if received value 0x00.
Description	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.
Message Primitives That Use This TLV	NetExit_MS_State_Change_Req

5.3.2.275 Duration Quota

Type	275
Length in octets	4
Value	Unsigned Integer representing seconds.
Description	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.
Parent TLV(s)	PPAQ

5.3.2.276 Duration Threshold

Type	276
Length in octets	4
Value	Unsigned Integer representing seconds.
Description	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.
Parent TLV(s)	PPAQ

5.3.2.277 Resource Quota

Type	277
Length in octets	4
Value	Unsigned Integer representing a resource measured in units.
Description	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.
Parent TLV	PPAQ

5.3.2.278 Resource Threshold

Type	278
Length in octets	4
Value	Unsigned Integer representing a resource measured in units.
Description	The semantics of this TLV follows those of the Volume Threshold and DurationThreshold.
Parent TLV	PPAQ

5.3.2.279 Update Reason

Type	279
Length in octets	1
Value	• Enumerator. The values are: 0x01 = Pre-initialization • 0x02 = Initial-Request • 0x03 = Threshold Reached • 0x04 = Quota Reached • 0x05 = TITSU Approaching • 0x06 = Remote Forced Disconnect • 0x07 = Client Service Termination • 0x08 = “Access Service” Terminated • 0x09 = Service not established • 0x0A = One-time Charging All other values are Reserved.
Description	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.
Parent TLV	PPAQ

5.3.2.280 Service-ID

Type	280
Length in octets	Variable
Value	The value field of this TLV is encoded as a string.
Description	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. A Service-Id is composed of two parts: tag and service identifier. The tag is encoded as an ASCII string. The tag for ALR is “ALR”. Other string values are reserved for future use. The service-identifier is represented as an IP 5-tuple (source address, source port, destination address, destination port, protocol). There are two Service-Ids for a local routing enabled service: one for the normal traffic and one for the local-routed traffic. The latter is identified by an ALR tag. Otherwise 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).
Parent TLV	PPAQ, Hotlining Context

5.3.2.281 Rating-Group-ID

Type	281
Length in octets	4
Value	Unsigned Integer representing the value of the Rating Group ID.
Description	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.
Parent TLV	PPAQ

5.3.2.282 Termination Action

Type	282
Length in octets	1
Value	Enumerator. The values are: • 0x00x01 = Terminate • 0x02 = Request more quota • 0x03 = Redirect/Filter All other values are Reserved.
Description	This TLV describes action to take when the PPS does not grant additional quota.
Parent TLV	PPAQ

5.3.2.283 Pool-ID

Type	283
Length in octets	4
Value	Unsigned Integer representing a Pool-ID.
Description	This TLV identifies the resource pool that the quota included in this PPAQ is associated with.
Parent TLV	PPAQ

5.3.2.284 Pool-Multiplier

Type	284
Length in octets	4
Value	32-bit unsigned integer.
Description	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.
Parent TLV	PPAQ

5.3.2.285 Prepaid Server

Type	285
Length in octets	4 (IPv4) or 16 (IPv6)
Value	The attribute consists of an unsigned integer.
Description	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.
Parent TLV	PPAQ

5.3.2.286 R3 Active Time

Type	286
Length	4
Value	32-bit unsigned Integer.
Description	The number of seconds the session was not in Idle Mode.
Parent TLV	Accounting Context

5.3.2.287 Interim Update Interval Remaining

Type	287
Length	4
Value	32-bit unsigned Integer.
Description	The number of seconds remaining in the current Interim Update Interval.
Parent TLV	Accounting Context

5.3.2.288 Number of UL Transport CIDs Support

Type	288
Length in octets	2
Value	16-bit unsigned integer.
Description	The number of uplink Transport CIDs supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.289 Number of DL Transport CIDs Support

Type	289
Length in octets	2
Value	16-bit unsigned integer.
Description	The number of downlink Transport CIDs supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.290 Classification/PHS Options and SDU Encapsulation Support

Type	290
Length in octets	2 or 4
Value	16 or 32-bit bitmask, as specified in the IEEE802.16e. It is named as 'CS type support' in IEEE802.16m.
Description	This TLV contains information of Classification/PHS options and SDU encapsulation which are supported by BS/ABS and MS/AMS, as defined in IEEE802.16e/m.
Parent TLV(s)	REG Context

5.3.2.291 Maximum Number of Classifier

Type	291
Length in octets	2
Value	16-bit unsigned integer.
Description	Maximum number of simultaneously admitted classification rules supported by BS/ABS and MS/AMS, as defined in IEEE802.16e/m.
Parent TLV(s)	REG Context

5.3.2.292 PHS Support

Type	292
Length in octets	1
Value	8-bit unsigned integer.
Description	This TLV indicates which type of PHS is supported by BS/ABS and MS/AMS, as defined in IEEE802.16e/m.
Parent TLV(s)	REG Context

5.3.2.293 ARQ Support

Type	293
Length in octets	1
Value	8-bit unsigned integer.
Description	This TLV indicates if ARQ is supported by BS/ABS and MS/AMS, as defined in IEEE802.16e/m.

Parent TLV(s)	REG Context

5.3.2.294 DSx Flow Control

Type	294
Length in octets	1
Value	8-bit unsigned integer.
Description	This TLV indicates how many concurrent transactions of DSx messages are supported by BS/ABS and MS/AMS, as defined in IEEE802.16e/m.
Parent TLV(s)	REG Context

5.3.2.295 Total Number of Provisioned Service Flows

Type	295
Length in octets	1
Value	8-bit unsigned integer.
Description	Total number of pre-provisioned service flows supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.296 Maximum MAC Data per Frame Support

<table>
<tr><td><b>Type</b></td><td colspan="2">296</td></tr>
<tr><td><b>Length</b></td><td colspan="2">Variable</td></tr>
<tr><td><b>Value</b></td><td colspan="2">Compound TLV</td></tr>
<tr><td><b>Description</b></td><td colspan="2">Maximum amount of MAC data per air frame supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.</td></tr>
<tr><td rowspan="3"><b>Elements</b></td><td><b>TLV Name</b></td><td><b>M/O</b></td></tr>
<tr><td>Maximum amount of MAC Level Data per DL Frame</td><td>M</td></tr>
<tr><td>Maximum amount of MAC Level Data per UL Frame</td><td>M</td></tr>
<tr><td><b>Parent TLV</b></td><td colspan="2">REG Context</td></tr>
</table>

5.3.2.297 Maximum amount of MAC Level Data per DL Frame

Type	297
Length in octets	2
Value	16-bit unsigned integer. A value of 0x0000 means unlimited.
Description	Maximum amount of downlink MAC data per air frame supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	Maximum MAC Data per Frame Support

5.3.2.298 Maximum amount of MAC Level Data per UL Frame

Type	298
Length in octets	2
Value	16-bit unsigned integer. A value of 0x0000 means unlimited.
Description	Maximum amount of uplink MAC data per air frame supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	Maximum MAC Data per Frame Support

5.3.2.299 Packing Support

Type	299
Length in octets	1
Value	8-bit unsigned integer.
Description	This TLV indicates if packing of fragments is supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.300 MAC ertPS Support

Type	300
Length in octets	1
Value	8-bit unsigned integer.
Description	This TLV indicates if ertPS scheduling type in the MAC layer is supported by BS/ABS and MS/AMS, as defined in IEEE802.16e/m.
Parent TLV(s)	REG Context

5.3.2.301 Maximum Number of Bursts Transmitted Concurrently to the MS

Type	301
Length in octets	1
Value	8-bit unsigned integer.
Description	Maximum number of bursts transmitted concurrently to the MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.302 HO Supported

Type	302
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This TLV indicates which type of handovers is supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.303 HO Process Optimization MS Timer

Type	303
Length in octets	1
Value	8-bit unsigned integer.
Description	The duration in frames the MS/AMS SHALL wait until receipt of the next unsolicited network reentry MAC management message, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.304 Mobility Features Supported

Type	304
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This TLV indicates if handover, sleep mode, and idle mode are supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	REG Context, RRM BS Info

5.3.2.305 Sleep Mode Recovery Time

Type	305
Length in octets	1
Value	8-bit unsigned integer.
Description	Number of frames required for the MS/AMS to switch from sleep mode to awake mode, as defined in IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.306 SF Type

Type	597
Length in octets	1
Value	Enumerator. The values are: 0x00 = ISF 0x01 = PPSF (except ISF) 0x02 = Dynamic Service Flow 0x03= Default Service Flow(DSF) All other values are Reserved.
Description	This attribute indicates service flow types of the service flow. This attribute may be included when the BS/ABS receives this message which include SF Info at the first time.
Parent TLV	SF Info

5.3.2.307 ARQ Ack Type

Type	307
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This TLV indicates which types of ARQ Ack types are supported by BS/ABS and MS/AMS, as defined in IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.308 MS HO Connections Parameters Proc Time

Type	308
Length in octets	1
Value	8-bit unsigned integer.
Description	Time in ms the MS/AMS needs to process information on connections during HO, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.309 MS HO TEK Proc Time

Type	309
Length in octets	1
Value	8-bit unsigned integer.
Description	Time in ms the MS/AMS needs to process TEK information during HO, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.310 MAC Header and Extended Sub-Header Support

Type	310
Length in octets	3
Value	24-bit bitmask, as specified in IEEE802.16e.
Description	This TLV indicates which types of MAC headers and sub-headers are supported by BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.311 System Resource Retain Timer

Type	311
Length in octets	2
Value	16-bit unsigned integer.
Description	System resource retain timer set by the BS/ABS during the initial network entry of MS/AMS, as defined in the IEEE802.16e/m.
Parent TLV(s)	REG Context

5.3.2.312 MS Handover Retransmission Timer

Type	312
Length in octets	1
Value	8-bit unsigned integer.
Description	MS Handover Retransmission Timer set by the BS/ABS during the initial network entry of MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.313 Handover Indication Readiness Timer

Type	313
Length in octets	1
Value	8-bit unsigned integer.
Description	MS Handover Indication Readiness Timer agreed by the BS/ABS and MS/AMS during the initial network entry of MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.314 BS Switching Timer

Type	314
Length in octets	1
Value	8-bit coded value, as specified in the IEEE802.16e.
Description	Minimum time from transmission of MOB_HO-IND at the serving BS/ABS until proper reception of Fast_Ranginin_IE at the target BS/ABS, as specified in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.315 Power Saving Class Capability

Type	315
Length in octets	2
Value	16-bit bitmask, as specified in the IEEE802.16e.
Description	This TLV indicates which types of power saving classes are supported by BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.316 Subscriber Transition Gaps

Type	316
Length in octets	2
Value	16-bit coded value, as specified in the IEEE802.16e.
Description	This TLV indicates the transition gap SSTTG and SSRTG for TDD and H-FDD SSs, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.317 Maximum Transmit Power

Type	317
Length in octets	4
Value	32-bit coded value, as specified in the IEEE802.16e/m.
Description	The maximum available power for BPSK, QPSK, 16-QAM, and 64-QAM constellations, as defined in the IEEE802.16e/m.
Parent TLV(s)	SBC Context

5.3.2.318 Capabilities for Construction and Transmission of MAC PDUs

Type	318
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	Indicates the capabilities for construction and transmission of MAC PDUs.
Parent TLV(s)	SBC Context

5.3.2.319 PKM Flow Control

Type	319
Length in octets	1
Value	8-bit unsigned integer.
Description	Maximum number of concurrent PKM transactions supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e/m.
Parent TLV(s)	SBC Context

5.3.2.320 Maximum Number of Supported Security Associations

Type	320
Length in octets	1
Value	8-bit unsigned integer.
Description	Maximum number of security association supported by the SS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.321 Security Negotiation Parameters

Type	321	
Length	Variable	
Value	Compound TLV	
Description	Security parameters that has been agreed between MS/AMS and BS/ABS and delivered in SBC-RSP/PKMv3 Keyagreement MSG#3 message during the initial network entry of MS/AMS.	
Elements	**TLV Name**	**M/O**

	PKM Version Support	O
	Authorization Policy Support	M
	MAC Mode	M
	PN Window Size	M
	SIZE of ICV	M
Parent TLV	SBC Context	

5.3.2.322 Void

5.3.2.323 MAC Mode

Type	323
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates which message authentication code mode is supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e/m. (CMAC only is defined in the IEEE02.16m).
Parent TLV(s)	Security Negotiation Parameters

5.3.2.324 PN Window Size

Type	324
Length in octets	2
Value	16-bit unsigned integer.
Description	Size of the receiver PN window for SAs and management connections supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e/m.
Parent TLV(s)	Security Negotiation Parameters

5.3.2.325 Extended Subheader Capability

Type	325
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	Extended subheader capability supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.326 HO Trigger Metric Support

Type	326
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e/m.
Description	This indicates which trigger metrics are supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e/m.
Parent TLV(s)	SBC Context(16e), REG Context(16m)

5.3.2.327 Current Transmit Power

Type	327
Length in octets	1
Value	8-bit unsigned integer.
Description	This indicates the transmitted power used for the burst which carried the SBC-REQ/AAI-SBC-REQ message, as defined in the IEEE802.16e/m.
Parent TLV(s)	SBC Context

5.3.2.328 OFDMA SS FFT Sizes

Type	328
Length in octets	1
Value	This indicates FFT size supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e/m.
Description	8-bit bitmask, as specified in the IEEE802.16e/m.
Parent TLV(s)	SBC Context

5.3.2.329 OFDMA SS demodulator

Type	329
Length in octets	variable
Value	Sets of 16-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates MS demodulator options supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.330 OFDMA SS modulator

Type	330
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates MS modulator options supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.331 The number of UL HARQ Channel

Type	331
Length in octets	1
Value	8-bit unsigned integer.
Description	The number of UL_HARQ channels supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.332 OFDMA SS Permutation support

Type	332
Length in octets	1
Value	8-bit unsigned integer.
Description	This indicates which OFDMA permutation modes are supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.333 OFDMA SS CINR Measurement Capability

Type	333
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates which channel quality measurement methods are supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.334 The number of DL HARQ Channels

Type	334
Length in octets	1
Value	8-bit unsigned integer.
Description	The number of DL_HARQ channels supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.335 HARQ Chase Combining and CC-IR Buffer Capability

Type	335
Length in octets	2
Value	16-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates if HARQ Chase Combining and CC-IR buffer are supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.336 OFDMA SS Uplink Power Control Support

Type	336
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates which power control methods for uplink are supported by MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.337 OFDMA SS Uplink Power Control Scheme Switching Delay

Type	337
Length in octets	1
Value	8-bit unsigned integer.
Description	Minimum number of frames that MS/AMS takes to switch between open-loop and closed-loop power control schemes, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.338 OFDMA MAP Capability

Type	338
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates which MAP options are supported by the BS/ABS and MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.339 Uplink Control Channel Support

Type	339
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates which uplink control channels are supported by MS/AMS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.340 OFDMA MS CSIT Capability

Type	340
Length in octets	2
Value	16-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates MS capability of supporting CSIT (UL sounding), as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.341 Maximum Number of Burst per Frame Capability in HARQ

Type	341
Length in octets	1
Value	8-bit coded value, as specified in the IEEE802.16e.
Description	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.
Parent TLV(s)	SBC Context

5.3.2.342 OFDMA SS demodulator for MIMO Support

Type	342
Length in octets	3
Value	24-bit bitmask, as specified in the IEEE802.16e.
Description	MIMO capability of MS demodulator, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.343 OFDMA SS modulator for MIMO Support

Type	343
Length in octets	2
Value	16-bit bitmask, as specified in the IEEE802.16e.
Description	MIMO capability of MS modulator, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.344 ARQ Context

Type	344	
Length in octets	Variable	
Value	Compound	
Description	Contains ARQ related information of the service flow.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**

	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
	ARQ SUB BLOCK SIZE	O
	MAXIMUM ARQ BUFFER SIZE	O
	MAXIMUM NON ARQ BUFFER SIZE	O
	ARQ ERROR DETECTION TIMEOUT	O
	ARQ FEEDBACK POLL RETRY TIMEOUT	O
	RECEIVER ARQ ACK PROCESSING TIME	O
Parent TLV(s)	SF Info	

1

2 ### 5.3.2.345 ARQ Enable

Type	345
Length in octets	1
Value	Enumerator. The values are: • 0x00 = ARQ Not Requested/Accepted • 0x01 = ARQ Requested/Accepted All other values are Reserved.
Description	Indicates whether ARQ is enabled or not for the corresponding service flow as defined in IEEE802.16e/m.
Parent TLV	SF Info

3 ### 5.3.2.346 ARQ WINDOW SIZE

Type	346
Length in octets	2
Value	This TLV is received over the R1 interface and SHALL follow the 802.16e/m definition.
Description	This parameter is negotiated upon connection setup or during operation as defined in IEEE802.16e/m.
Parent TLV	ARQ Context

5.3.2.347 ARQ RETRY TIMEOUT-Transmitter Delay

Type	347
Length in octets	2
Value	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
Description	This is the total transmitter delay, including sending and receiving delays and other implementation dependent processing delays as defined in IEEE802.16e.
Parent TLV	ARQ Context

5.3.2.348 ARQ RETRY TIMEOUT-Receiver Delay

Type	348
Length in octets	2
Value	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
Description	This is the total receiver delay, including receiving and sending delays and other implementation-dependent processing delays as defined in IEEE802.16e.
Parent TLV	ARQ Context

5.3.2.349 ARQ BLOCK LIFETIME

Type	349
Length in octets	2
Value	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
Description	Indicates the lifetime of ARQ block as defined in IEEE802.16e/m.
Parent TLV	ARQ Context

5.3.2.350 ARQ SYNC LOSS TIMEOUT

Type	350
Length in octets	2
Value	This TLV is received over the R1 interface and SHALL follow the 802.16e/m definition.
Description	Indicates the maximum time interval after which loss of synchronization is indicated as defined in IEEE802.16e/m.
Parent TLV	ARQ Context

5.3.2.351 ARQ DELIVER IN ORDER

Type	351
Length in octets	1
Value	As defined in IEEE802.16e.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
Parent TLV	ARQ Context

5.3.2.352 ARQ RX PURGE TIMEOUT

Type	352
Length in octets	2
Value	As defined in IEEE802.16e/m.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16e/m definition.
Parent TLV	ARQ Context

5.3.2.353 ARQ BLOCK SIZE

Type	353
Length in octets	2
Value	As defined in IEEE802.16e.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
Parent TLV	ARQ Context

5.3.2.354 RECEIVER ARQ ACK PROCESSING TIME

Type	354
Length in octets	1
Value	As defined in IEEE802.16e.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16e definition.
Parent TLV	ARQ Context

5.3.2.355 State

Type	355
Length in octets	Variable 1-253 octets
Value	Octet String
Description	State attribute as received in most recent message from AAA server.
Parent TLV(s)	MS Info

5.3.2.356 R3 Media Flow Description in SDP Format

Type	356
Length in octets	Variable
Value	<SDP string> is encoded as specified in IETF RFC 2327.
Description	This is a variable length string having SDP information. The <SDP string> is encoded as specified in IETF RFC 2327.
Parent TLV	R3 QoS descriptor

5.3.2.357 VolumeUsed

Type	357
Length in octets	4
Value	The attribute is an unsigned Integer representing a volume measured in kilo-bytes (1024 bytes).
Description	This TLV describes the total used volume (in octets) for both inbound and outbound traffic.
Parent TLV(s)	PPAQ

5.3.2.358 Time Stamp

Type	358
Length in octets	4
Value	32-bit unsigned integer.
Description	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.
Parent TLV(s)	BS Info

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		

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	

5.3.2.361 R3 Acct Session Time

Type	361
Length	4
Value	32-bit unsigned Integer
Description	The number of seconds the flow or session was active.
Parent TLV	Accounting Context

5.3.2.362 R3 Visited-Framed-IP-Address

Type	362
Length	4
Value	32-bit unsigned integer
Description	R3 Visited Framed-IP-Address.
Parent TLV	MS Authorization Context

5.3.2.363 R3 Visited-Framed-IPv6-Prefix

Type	363
Length	Variable
Value	0-128 bits
Description	R3 Visited Framed-IPv6-Prefix.
Parent TLV	MS Authorization Context

5.3.2.364 R3 Framed-Interface-Id

Type	364
Length	Variable
Value	8 bytes
Description	R3 Framed-Interface-Id.
Parent TLV	MS Authorization Context

5.3.2.365 R3 Visited-Framed-Interface-Id

Type	365
Length	Variable
Value	8 bytes
Description	R3 Visited-Framed-Interface-Id.
Parent TLV	MS Authorization Context

5.3.2.366 Delete MS Context Indication

Type	366
Length	1
Value	Unsigned Integer
Description	Indicates the release of the MS context.
Parent TLV	None

5.3.2.367 HO Authorization Policy Support

Type	367
Length in octets	1
Value	8-bit bitmask with the following values: • Bit #0 = RSA authorization • Bit #1 = EAP authorization • Bit #3 = HMAC supported • Bit #4 = CMAC supported • Bit #5 = 64-bit Short-HMAC • Bit #6 = 80-bit Short-HMAC • Bit #7 = 96-bit Short-HMAC All other bits are Reserved.
Description	This parameter is used to indicate that the authorization policy for the target BS/ABS is negotiated. Refer HO Authorization policy support in 802.16e(Cor2/D3) or 802.16m.
Parent TLV	BS Info

5.3.2.368 NSP ID

Type	368
Length in octets	3
Value	24-bits NSP ID
Description	Identifier of the NSP.
Parent TLV	MS Info

5.3.2.369 Idle Mode Exit Indicator

Type	369
Length in octets	1
Value	Enumerated. The values are: • 0x00 = Idle Mode Exit • 0x01 = MS in Idle Mode All other values are Reserved.
Description	Present in operations related to MS Idle Mode Exit and indicates whether MS/AMS's Serving ASN has MS Context.
Message Primitives that use this TLV	CMAC_Key_Count_Update, IM_Exit_State_Ind

5.3.2.370 Failure Indication Details

Type	370	
Length in octets	Variable	
Value	Compound	
Description	Contains details in addition to the information provided by the Failure Indication TLV. • 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.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	WiMAX message TLV position	O (Note 1)
Parent TLV(s)	None.	
Message Primitives that use this TLV	Any error message (i.e., Error Response message or Error Reflection message, see 3.5.2).	

Note 1: If this TLV is missing, the receiver SHALL ignore the Failure Indication Details TLV.

5.3.2.371 WiMAX® message TLV position

Type	371
Length in octets	3 * n (n >= 1)
Value	A sequence of n times - 2 bytes indicating a TLV Type (see section 5.3.1), to be called T_k below - an 8-bit unsigned integer, to be called R_k below where k = 0, …, n - 1.
Description	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, …, n-1); TLV_{n-1} is a top-level TLV; T_k is the Type of TLV_k (k = 0, …, 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 <= k < n-1)
Parent TLV	Failure Indication Details

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
Message Primitives That Use This TLV	Context_Rpt	

5.3.2.373 PMIP4 Context

Type	373	
Length in octets	Variable	
Value	Compound	
Description	MIP4 Information about the MS/AMS.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	MIP4 Info	M
Message Primitives That Use This TLV	Relocation_Complete_Rsp	

5.3.2.374 DNS IP Address

Type	374
Length in octets	Variable (either 4 or 16 bytes)
Value	IPv4 or IPv6 address.
Description	DNS server IP address
Parent TLV(s)	DHCP Proxy Info

5.3.2.375 Refresh IP Address Trigger

Type	375
Length in octets	1
Value	0 = Triggers BS/ABS to set the HO Process Optimization TLV/ Reentry Process Optimization settings in order for MS/AMS to perform "Full network entry without traffic IP address refresh (no optimization)" in RNG-RSP/AAI-RNG-RSP. 1 = Triggers BS/ABS to set the HO Process Optimization TLV/ Reentry Process Optimization settings in order for MS/AMS to perform "Traffic IP address refresh (with optimization) without full network entry" in RNG-RSP/AAI-RNG-RSP.
Description	Triggers BS/ABS to prompt MS/AMS for refreshing its IP address.
Message Primitives That Use This TLV	IM_Exit_State_Change_Rsp A WiMAX Release prior to 1.5 will not understand the meaning of this TLV.

5.3.2.376 Authorized Network Services

Type	376
Length in octets	4
Value	4 octet Bit Mask with the following values: • 0x00000001 – CMIP4 • 0x00000002 – PMIP4 • 0x00000004 – Simple IPv4 • 0x00000008 – CMIP6 • 0x00000010 – PMIP6 • 0x00000020 – Simple IPv6 • 0x00000040 – Simple ETH Service • 0x00000080 – MIP based ETH Service • 0x00000100 = L2 DHCP Relay[a] • The rest of the bits are reserved
Description	This TLV indicates the network service capabilities ASN is authorized to support
Parent TLV	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

Type	377
Length in octets	1
Value	4 octet Bit Mask with the following values: • Bit #0 – CMIP4 • Bit #1 – PMIP4 • Bit #2 – Simple IPv4 • Bit #3 – CMIP6 • Bit #4 – PMIP6 • Bit #5 – Simple IPv6 • Bit #6 – Simple ETH Service • Bit#7 – MIP based ETH Service • Bit#8 – L2 DHCP Relay[a] The rest of the bits are reserved
Description	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.
Parent TLV	MS Authorization Context

Note [a]: L2 DHCP Relay can be selected with either Simple ETH Service or MIP based ETH Service.

5.3.2.378 Void

5.3.2.379 Data Integrity Method

Type	437
Length in octets	4
Value	32-bit bitmask with the following values: • Bit #0 = M • Bit #1 = B • Bit #2 = F • Bit #3 = C • Bit #4 = D • Bit #5 = Sd • Bit #6 = Ua • Bit #7 = Ut All other bits are Reserved.
Description	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.
Parent TLV(s)	SF Info, BS Info

Internal structure of the value field appears as follows:

31								23								15								07							00
R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	R	Ut	Ua	Sd	D	C	F	B	M

Figure 5-1 – Structure of the Data Integrity Method bitmask

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.	The generic rule is the initiator of a transaction offers options and responder to the transaction selects options. Thus in Request messages all M, B and F bits may be set. In Response messages only one of them may be set. If none of these bits are set in the Response messages, then the HO data integrity feature SHALL NOT be supported for the handover.
B	If set means Buffering at the Anchor DP will (or is offered to) be applied.	
F	If set means Per-SF S-BS/ABS 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/ABS to BS/ABS Data Path Establishment will be applied.	If set, it implies that R8 data path setup for Buffer Switching is supported by Target BS/ABS and Serving BS/ABS. 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.
Sd	If set means ARQ Sync will (or is offered to) be applied in downlink.	Can be set independently of the other bits.
Ua	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.
Ut	If set means Uplink Reassembly at Target BS/ABS will (BS/ABS Buffer Switching with ARQ State and Buffer Synchronization) be applied.	
R	Reserved	

5.3.2.380 Data Integrity Applied

Type	438
Length in octets	1
Value	Enumerated. The values are: ● 0x00 = Not applied ● 0x01 = Applied All other values are Reserved.
Description	This TLV is used to indicate whether the Data Integrity Method should be applied to a specific Service Flow or not.
Parent TLV(s)	SF Info

5.3.2.381 Pointer BSN

Type	439
Length in octets	2
Value	Internally structured 16-bit value
Description	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.
Parent TLV(s)	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

Scope Value	Description
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

Type	440
Length in octets	Variable: from 3 to 10
Value	Bitmask
Description	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. The number of meaningful ARQ State fields equals the value of Map Length field plus one. 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.
Parent TLV(s)	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	

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

Value	Meaning for Uplink SF	Meaning for Downlink SF
0b00	Not Received State	Not Sent State
0b01	Ack Pending State	Outstanding
0b10	*Undefined*.	Waiting For Retransmission
0b11	Done State	Done State

5.3.2.383 Switching Data Path ID

Type	441
Length in octets	4
Value	Buffer Switching Data Path Identifier (e.g. GRE Key)
Description	Identifier for a buffer switching data path.
Parent TLV(s)	Data Path Info

5.3.2.384 MAC Source Address and Mask

Type	442
Length in octets	12
Value	A MAC Source Address/Mask pairs: (Src1, Smask) Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
Description	A MAC source address and mask. If this parameter is omitted, then comparison of the ethernet frame source address for this entry is irrelevant.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.385 MAC Destination Address and Mask

Type	443
Length in octets	12
Value	A MAC Destination Address/Mask pairs: (Dst1, Dmask) Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
Description	A MAC Destination address and mask. If this parameter is omitted, then comparison of the ethernet frame destination address for this entry is irrelevant.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.386 ETYPE/SAP

Type	444
Length in octets	3
Value	Ethernet Type or 802.2 SAP Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
Description	Ethernet Type or 802.2 SAP of the ethernet header.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.387 User Priority Range

Type	445
Length in octets	2
Value	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].
Description	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.
Parent TLV	Packet Classification Rule / Media Flow Description

5.3.2.388 Void

5.3.2.389 Void

5.3.2.390 C-VID>S-VID Mapping

Type	448
Length in octets	4
Value	C-VID,S-VID Note: Encoding of this TLV follows section 11.13.18.3 of IEEE802.16-2009 [13].
Description	The value of the field specifies a mapping between a C-VID and a S-VID
Parent TLV	VLAN Tag Processing Rule

5.3.2.391 C-VLAN Priority Setting

Type	449
Length in octets	2
Value	Bitfield; the bits have the following meanings: • 0x0000 = forward the p_bits without modification • 0x001x = drop frames with p_ bits set to a higher value than x • 0x002x = set p_bits to x when p_bits set to a higher value than x • 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. Other values reserved Note: One of the bitfield definitions can be assigned at a time.
Description	Defines the setting of the priority_bits in the C-VLAN tag in the upstream direction.
Parent TLV	VLAN Tag Processing Rule

5.3.2.392 VLAN ID Assignment

Type	450
Length in octets	2
Value	Bitfield; the bits have the following meaning: • 0x0000 = forward VLAN tags without modification • 0x0010 = remove S-VID in downstream direction • 0x0020 = remove C-VID and S-VID, if present, in downstream direction • 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 • 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 • 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 • 0x040x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C->S-VID Mapping table and S-p_bits set to x If no entry exists for a particular C-VID in the C-VID>S-VID Mapping table, the S-VID is set to 0 • 0x0480 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C->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>S-VID Mapping table, the S-VID is set to 0 Other values reserved Note: One downstream rule can be combined (ORed) with one upstream rule.
Description	Defines the processing of the VLAN tags in both the upstream and downstream direction.
Parent TLV	VLAN Tag Processing Rule

5.3.2.393 SVLAN ID

Type	451
Length in octets	2
Value	SVLAN ID Note: Encoding of the VLAN value follows section 11.13.18.3 of IEEE802.16-2009 [13].
Description	The value of the field specifies a SVLAN ID.
Parent TLV	VLAN Tag Processing, Packet Classification Rule/Media Flow Descriptor

5.3.2.394 CVLAN ID

Type	452
Length in octets	2
Value	CVLAN ID Note: Encoding of the VLAN ID value follows section 11.13.18.3 of IEEE802.16-2009 [13].
Description	The value of the field specifies a CVLAN ID.
Parent TLV	VLAN Tag Processing, Packet Classification Rule/Media Flow Descriptor

5.3.2.395 LocalConfigInfo

Type	453
Length in octets	2+n
Value	String of length n containing arbitrary information The meaning of the information in LocalConfigInfo is subject of static configuration agreements between NAP and NSP.
Description	Local configuration information for preprovisioned R3 data path (Simple Ethernet)
Parent TLV	VLAN Tag Processing Rule

5.3.2.396 VLANTagProcessingRuleID

Type	454
Length in octets	2
Value	Short-Unsigned
Description	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.
Parent TLV	VLAN Tag Processing Rule

5.3.2.397 VLAN Tag Processing Rule

Type	455	
Length in octets	Variable	
Value	Compound	
Description	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.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	VLANTagProcessingRuleID	M
	VLAN Priority setting	M
	VLAN ID Assignment	O
	CVLAN ID	O
	SVLAN ID	O
	C-VID>S-VID Mapping	O[1]
	LocalConfigInfo	O[2]
Parent TLV	SF Info	

[1] This Sub-TLV MAY appear multiple times in the TLV

[2] LocalConfigInfo is not used in the case of MIP based Ethernet Services.

5.3.2.398 Uplink R3 GRE Key

Type	456
Length in octets	4
Value	Uplink GRE Key
Description	GRE key used to mark the uplink traffic on the R3 interface when GRE encapsulation is used over R3.
Parent TLV	MIP4 Info

5.3.2.399 Downlink R3 GRE Key

Type	457
Length in octets	4
Value	Downlink GRE Key
Description	GRE key used to mark the downlink traffic on the R3 interface when GRE encapsulation is used over R3.
Parent TLV	MIP4 Info

5.3.2.400 Hotlining Context

Type	458	
Length	Variable	
Value	Compound	
Description	Carries the Hotlining Context from PPC to HLD; if both are not Collocated.	
Elements	**TLV Name**	**M/O**
	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
Message Primitives that Carries this TLV	Hotlining Req, Hotlining Rsp	

5.3.2.401 R3 Hotline-Profile-ID

Type	459
Length	Octet String
Value	String representing a Hot-Line profile.
Description	ID to uniquely identify the user's Hot-Line profile. See 5.4.2.53 for more details.
Parent TLV	Hotlining Context

5.3.2.402 R3 HTTP-Redirection-Rule

Type	460
Length	Variable
Value	An string formatted as per IPFilterRule specified by RFC 3588 [55] with some exception: See 5.4.2.54 for more details.
Description	Instructs the Hot-Lining Device where to redirect HTTP flows.
Parent TLV	Hotlining Context

5.3.2.403 R3 IP-Redirection-Rule

Type	461
Length	Variable
Value	An string formatted as per IPFilterRule specified by RFC 3588 [55] with some exception: See 5.4.2.55 for more details.
Description	Used to specify which packet flow to redirect and where to redirect it.
Parent TLV	Hotlining Context

5.3.2.404 R3 NAS-Filter-Rule

Type	462
Length	Variable
Value	The String field is one or more octets.
Description	As defined by RFC 4849 [1]
Parent TLV	Hotlining Context

5.3.2.405 R3 Hotline-Session-Timer

Type	463
Length	4
Value	Unsigned Integer representing a time in seconds. A value of zero means infinity.
Description	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.
Parent TLV	Hotlining Context

5.3.2.406 Remaining Hotline Session Timer

Type	464
Length	4
Value	Unsigned Integer representing a time in seconds. A value of zero means infinity.
Description	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.
Parent TLV	Hotlining Context

5.3.2.407 R3 Hotline-Indication

Type	465
Length	Length of String
Value	A string value which is to be opaque.
Description	Indicates that the flow is Hot-Lined. See 5.4.2.24 for more details.
Parent TLV	Hotlining Context

5.3.2.408 R3 Hotlining Capability

Type	466
Length	1
Value	Unsigned Integer.
Description	Octet interpreted as a bit map with the following values: • Bit#0 = Profile-based Hot-Lining is supported (using the Hotline-Profile-ID VSA). • Bit#1 = Rule-based Hot-Lining is supported using NAS-Filter-Rule. • Bit#2 = Hot-Lining HTTP Redirection is supported. • Bit#3 = Rule-based Hot-Lining is supported using IP-Redirection rule. Other values reserved A value of zero (none of the bits being set) or the omission of this subTLV means that Hot-Lining is not supported. Bit#2 and Bit#3 SHALL always be set.
Parent TLV	R3 WiMAX Capability

5.3.2.409 DSCP

<table>
<tr><td><b>Type</b></td><td>496</td></tr>
<tr><td><b>Length</b></td><td>1</td></tr>
<tr><td><b>Value</b></td><td>Unsigned Octet representing the DSCP field as defined in RFC2474 [30]
DSCP field as defined in rfc2475 [31]
<pre>
    0   1   2   3   4   5   6   7
  +---+---+---+---+---+---+---+---+
  | DSCP | CU |
  +---+---+---+---+---+---+---+---+

    DSCP: differentiated services codepoint
    CU: currently unused
</pre></td></tr>
<tr><td><b>Description</b></td><td>Differentiated services codepoint as defined in RFC 2474 [30]. 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).
Used to mark the IP packets of the flow. See RFC3246 [47], RFC2597 [35] and RFC4595 [77] for recommended values.</td></tr>
<tr><td><b>Parent TLV</b></td><td>QoS Parameters</td></tr>
</table>

5.3.2.410 PHY Mode ID

Type	497
Length	2
Value	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/m[11].
Description	This TLV indicates which PHY mode SHALL be used at a BS/ABS. It SHALL be present in the message when the phy mode of a BS/ABS is different from the recipient BS/ABS, as defined in IEEE802.16e/m [11].
Parent TLV	RRM BS Info

5.3.2.411 Scheduling Service Supported

Type	498
Length	1
Value	8-bit bitmap, as specified in the IEEE802.16e/m [11].
Description	This TLV indicates which scheduling service types can be supported at the BS/ABS. Bitmap to indicate if BS/ABS supports a particular scheduling service. 1 indicates support, 0 indicates not support: Bit #0: Unsolicited grant service (UGS) Bit #1: Real-time polling service (rtPS) Bit #2: Non-real-time polling service (nrtPS) Bit #3: Best effort (BE) service Bit #4: Extended real-time polling service (ertPS) Bits #5–7: Reserved; SHALL be set to zero. If the value of bit 0 through bit 4 is 0b00000, it indicates no information on service available.
Parent TLV	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
Parent TLV(s)	Anchor MM Context	

5.3.2.413 LMA IPv6 Address

Type	426
Length in octets	16
Value	The Identifier in format of 16-octet IPv6 Address.
Description	IPv6 address of the LMA.
Parent TLV(s)	PMIP6 Info

5.3.2.414 LMA IPv4 Address

Type	427
Length in octets	4
Value	The Identifier in format of 4-octet IPv4 Address.
Description	IPv4 address of the LMA.
Parent TLV(s)	PMIP6 Info

5.3.2.415 MAG IPv6 Address

Type	428
Length in octets	16
Value	The Identifier in format of 16-octet IPv4 Address.
Description	IPv6 address of the LMA
Parent TLV(s)	PMIP6 Info

5.3.2.416 Home Network Prefix (HNP)

Type	429
Length in octets	0-16 octets
Value	Variable size IPv6 address prefix
Description	The IPv6 home network address prefix that is assigned to a MS/AMS for PMIP6 mobility
Parent TLV(s)	PMIP6 Info

5.3.2.417 PMIP6 Security Indicator

Type	430
Length in octets	1
Value	Indicates whether in-band signaling protection is used for PMIP6
Description	Enumerator. The values are: • 0x00 = Lower-layer security • 0x01 = In-band security
Parent TLV(s)	PMIP6 Info

5.3.2.418 DHCP Proxy Type

Type	431
Length in octets	1
Value	Indicates IP version designation of the DHCP Proxy (IPv4 or IPv6)
Description	Enumerator. The values are: • 0x00 = DHCPv4 Proxy • 0x01 = DHCPv6 Proxy
Parent TLV(s)	DHCP Proxy Info

5.3.2.419 PMIP6 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	

5.3.2.420 MAG-LMA-PMIP6 Key

Type	433
Length in octets	20
Value	160-bit unsigned integer.
Description	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.
Parent TLV(s)	PMIP6 Security Info

5.3.2.421 MAG-LMA-PMIP6 SPI

Type	434
Length in octets	4
Value	32-bit unsigned integer.
Description	Key ID of MAG-LMA-PMIP6 key. It should be equal to the SPI of PMIP6-RK.
Parent TLV(s)	PMIP6 Security Info

5.3.2.422 MAG-LMA-PMIP6-Lifetime

Type	435
Length in octets	4
Value	32-bit unsigned integer.
Description	Time for MAG-LMA-PMIP6 key remaining valid. This is provided to the MAG by the anchor Authenticator for PMIP6 key context transfer.
Parent TLV(s)	PMIP6 Security Info

5.3.2.423 Mobility Access Classifier

Type	499
Length in octets	1
Value	1 = Fixed 2 = Nomadic 3 = Mobile 4-255= Reserved
Description	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.
Parent TLV(s)	MS Info, Information

5.3.2.424 Reattachment Zone

Type	500
Length in octets	Variable
Value	List of BS ID.
Description	BS ID List where a fixed or nomadic MS/AMS is allowed to reattach or handoff to.
Parent TLV(s)	BS Info, MS Info

5.3.2.425 BS Location

Type	501
Length in octets	Variable
Value	Octet String
Description	BS Location info which may be described as Lat/Long/Sector/carrier information of BS/ABS.
Parent TLV(s)	BS Info

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
Message Primitives That Use This TLV	Capability_Req, Capability_Rsp, Capability_Ack	

5.3.2.427 R4R6R8 WiMAX® Release

Type	505
Length in octets	Variable
Value	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”.
Description	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 ‘1.6’.
Parent TLV(s)	WiMAX® Release Info

5.3.2.428 Capabilities Info

Type	506	
Length in octets	Variable	
Value	Compound	
Description	A list of optional capabilities supported by a network node for a given WiMAX Release.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	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
	Support-of- Packet-Flow-Operation-Policy	O
	Support-of-IPv6	O
Parent TLV(s)	WiMAX® Release Info	

Note: “ASN-GW ROHC Capability” is defined in the R1.5 ROHC Standalone Specification [8], section 7.3.2.7.

5.3.2.429 Support-of-MCBCS

Type	507
Length in octets	1
Value	0x00 = MCBCS is not supported 0x01 = MCBCS-DSx is supported 0x02 = MCBCS-Appl is supported All other values are Reserved.
Description	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.
Parent TLV(s)	Capabilities Info

5.3.2.430 Support-of-HO-DI

Type	508
Length in octets	1
Value	0x00 = Handover Data Integrity is not supported 0x01 = Handover Data Integrity is supported All other values are Reserved.
Description	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.
Parent TLV(s)	Capabilities Info

5.3.2.431 Support-of-dMAC

Type	509
Length in octets	1
Value	0x00 = Duplicate MS Context per MS/AMS MAC address is not supported 0x01 = Duplicate MS Context per MS/AMS MAC address is supported All other values are Reserved.
Description	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/Ack message, it indicates whether Duplicate MS Context per MS/AMS MAC address is supported by the sending node.
Parent TLV(s)	Capabilities Info

5.3.2.432 Support-of-Accounting

Type	510
Length in octets	1
Value	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.
Description	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.
Parent TLV(s)	Capabilities Info

5.3.2.433 Support-of-IMS-ES

Type	511
Length in octets	1
Value	0x00 = IMS and Emergency Service is not supported 0x01 = IMS and Emergency Service is supported All other values are Reserved.
Description	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.
Parent TLV(s)	Capabilities Info

5.3.2.434 Support-of-PCC-QoS

Type	512
Length in octets	1
Value	0x00 = PCC-QoS is not supported 0x01 = PCC-QoS is supported All other values are Reserved.
Description	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.
Parent TLV(s)	Capabilities Info

5.3.2.435 Support-of-EtherServ

Type	513
Length in octets	1
Value	0x00 = EtherServ is not supported 0x01 = EtherServ is supported All other values are Reserved.
Description	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.
Parent TLV(s)	Capabilities Info

5.3.2.436 Support-of-LBS

Type	514
Length in octets	1
Value	0x00 = LBS is not supported 0x01 = LBS is supported All other values are Reserved.
Description	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.
Parent TLV(s)	Capabilities Info

5.3.2.437 Support-of-FixedNom

Type	515
Length in octets	1
Value	0x00 = FixedNom is not supported 0x01 = FixedNom is supported All other values are Reserved.
Description	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.
Parent TLV(s)	Capabilities Info

5.3.2.438 Support-of-Hotlining

Type	516
Length in octets	1
Value	1 octet Bit Mask with the following values: 0x00 = not allowed 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.
Description	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. Bit 2 and Bit 3 MUST be set. A value of 0x00 MUST never be used.
Parent TLV(s)	Capabilities Info

5.3.2.439 Support-of-RRM

Type	517
Length in octets	1
Value	0x00 = RRM is not supported 0x01 = RRM is supported All other values are Reserved.
Description	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)
Parent TLV(s)	Capabilities Info

Note: Additional values might be used for indicating support for specific RRM procedures, e.g. Neighbor BS Status Update procedure or the Spare Capability reporting procedure.

5.3.2.440 R6_Context_ID

Type	572
Length in octets	12
Value	96 bit Unsigned Integer
Description	Unique session identifier for an R6 context of a MS/AMS that is assigned by the BS/ABS and is used in the BS/ABS and Authenticator to separate parallel R6 messages for one or several MS/AMSes with the same MAC address during network entry. The R6_Context_ID is unique for all such contexts handled at a specific BS/ABS. Uniqueness across the ASN can be guaranteed in the Authenticator by using the combination of R6_Context_ID and BS_ID. The value ‘0’ is used by the ASN-GW to indicate that no value has been assigned yet to the R6_Context_ID. If the duplicate MAC address detection feature is not supported by the BS/ABS, the BS/ABS assigns a value of ‘0’ to the R6_Context_ID. R6_Context_ID is placed after the message header according to the rules specified in section 3.2.
Parent TLV(s)	None.

5.3.2.441 R3 WiMAX®-Release

Type	573
Length in octets	Variable
Value	Octet String
Description	WiMAX release negotiated during Network Entry for the respective session.
Parent TLV(s)	R3 WiMAX® Capability

5.3.2.442 Last Reset Time

Type	574
Length in octets	4
Value	The least significant 32-bits of Timestamp in UTC format. The LRT Timestamp will be in 24 hour format with granularity in seconds since January 1, 1970 00:00 UTC.
Description	The timestamp of the last NE boot up. The NE generating this value SHOULD ensure the value is unique over the NE restarts.
Parent TLV(s)	Keep-alive Req, Keep-alive Rsp

5.3.2.443 Health Status

Type	575	
Length in octets	Variable	
Value	Compound	
Description	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.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Status	M[a] [b]
	Reported Node ID	O [c]
	Reference Last Reset Time	O [d]
	Function ID	O [b]
Message Primitives that use this TLV	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.

5.3.2.444 Status

Type	576
Length in octets	1
Value	Enumerator. The values are: • 0x00 = Operating Normally • 0x01 = Failed • 0x02 = Shutting Down All other values are Reserved.
Description	The status of the message originator or the reported Network Entity as indicated by the presence of the Reported Node ID TLV.
Parent TLV(s)	Health Status

5.3.2.445 Reported Node ID

Type	577
Length in octets	Variable (could be of three fixed sizes: 4, 6 and 16 octets)
Value	The Identifier might be in format of either 4-octet IPv4 Address, 6-octet IEEE 802.16 ID value or 16-octet IPv6 Address. The length defines also the format of the Identifier.
Description	The Identity of the reported Network Entity.
Parent TLV(s)	Health Status

5.3.2.446 Reference Last Reset Time

Type	578
Length in octets	4
Value	The least significant 32-bits of Timestamp in UTC format
Description	The timestamp of the last boot up for the reported Network Entity. The use of this TLV is FFS.
Parent TLV(s)	Health Status

5.3.2.447 Function ID

Type	579
Length in octets	1
Value	Enumerator. The values are: • 0x00 = ALL (default) All other values are Reserved.
Description	Indicates the reported Functional Entity as defined for WiMAX ASN GW – Authenticator, Anchor GW or PC. If missing, the Default value is assumed.
Parent TLV(s)	Health Status

5.3.2.448 ARQ Window Info

Type	580	
Length in octets	Variable	
Value	Compound	
Description	ARQ window information parameters which shall be used to deliver ARQ states of each SF at the Serving BS/ABS to the Target BS/ABS.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Starting ARQ BSN	M
	Last ARQ BSN	M
	Valid ARQ BSN	O
	Reset Status	O
Parent TLV(s)	SF Info	

5.3.2.449 Starting ARQ BSN

Type	581
Length in octets	2
Value	16-bit Integer. Block Sequence Number, as defined in IEEE802.16e/m
Description	Identifies the Block Sequence Number of the first ARQ Block in the ARQ window of a particular SF.
Parent TLV(s)	ARQ Window Info

5.3.2.450 Last ARQ BSN

Type	582
Length in octets	2
Value	16-bit Integer. Block Sequence Number, as defined in IEEE802.16e/m
Description	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.
Parent TLV(s)	ARQ Window Info

5.3.2.451 Valid ARQ BSN

Type	583
Length in octets	2
Value	16-bit Integer. Block Sequence Number, as defined in IEEE802.16e/m
Description	This TLV indicates whether the ARQ Discard was outstanding at the Serving BS/ABS before HO indication from MS is received. If this TLV is included, the Target BS/ABS shall issue a ARQ_DISCARD MAC management message to the MS/AMS for Blocks, whose sequence numbers are less than the specified value, after the completion of MS/AMS HO.

Parent TLV(s)	ARQ Window Info

5.3.2.452 Reset Status

Type	584
Length in octets	1
Value	Enumerator: The values are: • 0x00 = No ARQ RESET was issued at the Serving BS/ABS before HO • 0x01 = ARQ_RESET was outstanding at the Serving BS/ABS before HO All other values are Reserved.
Description	This TLV indicates whether the ARQ Reset was outstanding at the Serving BS/ABS before HO indication from MS/AMS is received. If this TLV is set, the Target BS/ABS shall issue a ARQ_RESET MAC management message to the MS/AMS, right after the completion of MS/AMS HO.
Parent TLV(s)	ARQ Window Info

5.3.2.453 HARQ Context

Type	585	
Length in octets	Variable	
Value	Compound	
Description	Contains HARQ related information for the service flow. If TLV is missing, then HARQ is disabled in the service flow.	
Elements (Sub-TLVs)	**TLV Name**	**M/O**
	Direction	O
	HARQ Enable	O
	HARQ Channel Mapping	O
	PDU SN extended subheader for HARQ reordering	O
Parent TLV(s)	SF Info, SBC Context	

5.3.2.454 HARQ Enable

Type	586
Length in octets	1
Value	This TLV is received over the R1 interface and shall follow the 802.16e definition. In case of R1 inferface in ABS(MZone) HARQ SHALL be enabled as defined in IEEE802.16m.
Description	As defined in IEEE802.16e. If TLV is missing, then HARQ is disabled in the service flow.
Parent TLV(s)	HARQ Context

5.3.2.455 HARQ Channel Mapping

Type	587
Length in octets	Variable
Value	This TLV is received over the R1 interface and shall follow the 802.16e/m definition.
Description	As defined in IEEE802.16e/m. If TLV is missing, then all HARQ channels are used in the service flow.
Parent TLV(s)	HARQ Context

5.3.2.456 PDU SN extended subheader for HARQ reordering

Type	588
Length in octets	1
Value	This TLV is received over the R1 interface and shall follow the 802.16e definition.
Description	As defined in IEEE802.16e. If TLV is missing, then PDU SN is not used in the service flow.
Parent TLV(s)	HARQ Context

5.3.2.457 Priority Indication

Type	589
Length in octets	1
Value	Bit 0: Priority Indicator (PI), where value = 1 indicates the priority service is enabled and value = 0 indicates the priority service disabled. Bit 1: Reserved Bit 2: Pre-emption Capability (PC), where value = 0 indicates that pre-emption is allowed and value = 1 indicates that pre-emption is not allowed. Bit 3: Pre-emption Vulnerability (PV), where value = 0 indicates that pre-emption is enabled and value = 1 indicates that pre-emption is disabled. Bits 4-7: constitute the Allocation Priority sub-field, which provides 15 priority levels/ (values 1 to 15). The value 1 represents the highest level of priority. The value 0 is reserved.
Description	Priority indication for emergency purposes, including ETS.
Parent TLV(s)	R3 QoS Descriptor, QoS Parameters

5.3.2.458 IP Address of Requesting BS

Type	596
Length in octets	4 (IPv4) or 16 (IPv6)
Value	IP Address
Description	An IP Address of the requesting BS/ABS. Must be included in an R4 MS Pre-Attachment Request message.
Parent TLV(s)	BS Info

5.3.2.459 SF Operation Policy

Type	598
Length in octets	1
Value	The bitmap is used to indicate SF Operation policies as follows: Bit-0 = "0" - airlink encryption shall be disabled for the given SF. Bit-0 = "1" - airlink encryption shall be enabled for the given SF. If the ASN has indicated the support of per SF airlink encryption on/off capability but this TLV is missing, it implies that the SF operation policies are based on local policies. Note that, the airlink encryption policy for the service flow is set during the service flow establishment procedure and cannot be changed during the lifetime of the service flow. All other values are "reserved". The sender shall set the reserved bit to "0", and the receiver shall ignore the reserved bit.
Description	Bitmap. The value of this optional parameter, if supported and included, is to instruct the serving ASN to apply for the service flow related operation policy for a given service flow.
Parent TLV(s)	SF Info

5.3.2.460 Support-of-Packet-Flow-Operation-Policy

Type	599
Length in octets	1
Value	This TLV is designed for indicating the support of the operation policy capability for the service flow. 0x00 = per SF airlink encryption on/off capability is NOT supported for the given SF 0x01 = per SF airlink encryption on/off capability is supported for the given SF If this TLV is not present, it implies the sender does NOT support the per SF airlink encryption on/off capability and the airlink encryption for the given service flow is a local implementation policy of the ASN. All other values are Reserved.
Description	When this TLV is included in the Capabilities_Info TLV in the Capability_Req message, it indicates that Packet-Flow-Operation-Policy is supported by the sending node. This TLV is included in the Capabilities_Info TLV in the Capability_Rsp message only if previously sent by the sending node. When present it indicates that Packet-Flow-Operation-Policy is also supported by the receiving node.
Parent TLV(s)	Capabilities Info

5.3.2.461 Support-of-IPv6

Type	602
Length in octets	1
Value	0x00 = IPv6 is not supported 0x01 = IPv6 is supported All other values are Reserved.
Description	When this TLV is included in the Capabilities_Info TLV in Capability_Req/Rsp/ message, it indicates whether IPv6 is supported by the sending node.
Parent TLV(s)	Capabilities Info

5.3.2.462 MCA flow control

Type	603
Length in octets	1
Value	8-bit value, as specified in the IEEE802.16e.
Description	The MCA flow control field indicates the maximum number of concurrent MCA transactions, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.463 Multicast polling group CID

Type	604
Length in octets	1
Value	8-bit value, as specified in the IEEE802.16e.
Description	The field indicates the maximum number of simultaneous multicast polling groups to which the SS is capable of belonging, as defined in the IEEE802.16e.
Parent TLV(s)	REG Context

5.3.2.464 PKM version support

Type	605
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e. Bit 0: PKM version 1 Bit 1: PKM version 2 Bits 2–7: Reserved; shall be set to 0.
Description	The PKM Version Support field indicates a PKM version, as defined in the IEEE802.16e.
Parent TLV(s)	Security Negotiation Parameters

5.3.2.465 Association type support

Type	606
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	The Association Type Support field indicates the association level supported by the MS or the BS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.466 OFDMA multiple DL burst profile capability

Type	607
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates DL/UL Burst Profile that shall be used for MS and BS, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.467 SDMA Pilot capability

Type	608
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16e.
Description	This indicates SDMA pilot pattern support for AMC zone, as defined in the IEEE802.16e.
Parent TLV(s)	SBC Context

5.3.2.468 SN Feedback Enabled field

Type	609
Length in octets	1
Value	8-bit value, as specified in the IEEE802.16e.
Description	The SN Feedback Enabled field indicates whether SN feedback is enabled for the given connection, as defined in the IEEE802.16e.
Parent TLV(s)	SF Info

5.3.2.469 FSN Size

Type	610
Length in octets	1
Value	8-bit value, as specified in the IEEE802.16e.
Description	The FSN Size field indicates the size of the FSN for the connection that is being setup, as defined in the IEEE802.16e.
Parent TLV(s)	SF Info

5.3.2.470 IPv6 Flow Label

Type	611
Length in octets	3
Value	IPv6 Flow Label.
Description	The value of this field specifies a matching value for the IPv6 Flow Label field. As the Flow Label field has a length of 20 bits, the first 4 bits of the most significant byte shall be set to 0x0 and disregarded.
Parent TLV(s)	Packet Classification Rule / Media Flow Description

5.3.2.471 FID

Type	612
Length in octets	1
Value	4-bit unsigned integer.
Description	FID definition as per 802.16m.
Parent TLV(s)	SF Info

5.3.2.472 MSID*

Type	613
Length in octets	6
Value	
Description	Hash of AMS MAC address used to protect the real MSID in Rel.2.0 operation
Parent TLV(s)	MS Info,

5.3.2.473 STID

Type	614
Length in octets	2
Value	
Description	Station identifier which a Serving ABS assigns to the AMS uniquely in Rel.2.0 operation.
Parent TLV(s)	MS Info,

5.3.2.474 DCR Context

Type	615	
Length in octets	Variable	
Value	Compound	
Description	Contains DCR mode related information for the AMS	
Elements (Sub-	**TLV Name**	**M/O**

TLVs)	Combined Resource Indicator	O
	>CS Type	CM
	SBC Context	O
	>Maximum Transmit Power	CM
	>Security Negotiation Parameters	CM
	>>Authorization Policy Support	CM
	>>MAC Mode	CM
	>>PN Window Size	CM
	>OFDMA SS FFT Sizes	CM
	>CAPABILITY_INDEX	O
	>DEVICE_CLASS	O
	>CLC Request	O
	>Long TTI for DL	O
	>UL sounding	O
	>OL Region	O
	>DL resource metric for FFR	O
	>Max. Number of streams for SU-MIMO in DL MIMO	O
	>Max. Number of streams for MU-MIMO in MS point of view in DL MIMO	O
	>DL MIMO mode	O
	>feedback support for DL	O
	>Subband assignment A-MAP IE support	O
	>DL pilot pattern for MU MIMO	O
	>Number of Tx antenna of AMS	O
	>Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)	O
	>Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)	O
	>UL pilot pattern for MU MIMO	O
	>UL MIMO mode	O
	>Modulation scheme	O
	>UL HARQ buffering capability	O
	>DL HARQ buffering capability	O
	>AMS DL processing capability per sub-frame	O
	>AMS UL processing capability per sub-frame	O
	>FFT size(2048/1024/512)	O

	>Authorization policy support	O
	>Inter-RAT Operation Mode	O
	>Supported Inter-RAT type	O
	>MIH Capability Supported	O
	>Visited NSP ID	O
	REG Context	O
	>Classification/PHS Options and SDU Encapsulation Support	O
	>Maximum Number of Classifier	O
	>PHS Support	O
	>MAXIMUM_ARQ_BUFFER_SIZE	O
	>MAXIMUM_NON_ARQ_BUFFER_SIZE	O
	>Multicarrier capabilities	O
	>Zone Switch Mode Support	O
	>Capability for supporting A-GPS Method for LBS service	O
	>Interference mitigation supported	O
	>E-MBS capabilities	O
	>Channel BW and Cyclic prefix	O
	>frame configuration to support legacy R1.0	O
	>Persistent Allocation support	O
	>Group Resource Allocation support	O
	>Co-located coexistence capability support	O
	>HO Trigger Metric Support	O
	>EBB Handover support	O
	>Minimal HO Reentry Interleaving Interval	O
	>Capability for sounding antenna switching support	O
	>Antenna configuration for sounding antenna switching	O
	>ROHC support	O
	>Host-Configuration-Capability-Indicator	M
	>AMS initiated aGP Service Adaptation Capability:	O
Parent TLV(s)		

5.3.2.475 CRID

Type	616
Length in octets	9
Value	The 48 most significant bits (6 octets) comprise the Authenticator ID that is serving the AMS and the 24 least significant bits (3 octets) comprise a unique value per AMS
Description	The CRID value per the definition in section 4.23.2
Parent TLV(s)	MS Info,

5.3.2.476 IPv4-Host-Address

Type	617
Length in octets	4
Value	
Description	Used if FIAA is applied.
Parent TLV(s)	MS Info

5.3.2.477 IPv6-Home-Network-Prefix

Type	618
Length in octets	8
Value	
Description	Used if FIAA is applied.
Parent TLV(s)	MS Info

5.3.2.478 Additional-Host-Configurations

Type	619
Length in octets	variable
Value	
Description	Used if FIAA is applied.
Parent TLV(s)	MS Info

5.3.2.479 Basic CID

Type	620
Length in octets	2
Value	
Description	Basic CID assigned by the old Serving BS. An AMS is uniquely defined by old Serving BS ID and its Basic CID in case of uncontrolled handover from the LZone of an ABS to the MZone,
Parent TLV(s)	MS Info

5.3.2.480 Deregistration ID

Type	621
Length in octets	3
Value	
Description	Deregistration ID assigned to the AMS for Idle mode entry in MZone of ABS
Parent TLV(s)	Paging Information

5.3.2.481 current Paging Cycle

Type	622
Length in octets	1
Value	
Description	PAGING_CYCLE applied to the AMS, which identifies uniquely an AMS in idle mode with combination with the current Paging Offset, the current Paging Group ID and the current Deregistration ID.
Parent TLV(s)	Paging Information

5.3.2.482 current Paging Offset

Type	623
Length in octets	2
Value	
Description	PAGING_OFFSET applied to the AMS, which identifies uniquely an AMS in idle mode with combination with the current Paging Cycle, the current Paging Group ID and the current Deregistration ID.
Parent TLV(s)	Paging Information

5.3.2.483 current Deregistration ID

Type	624
Length in octets	3
Value	
Description	Deregistration ID assigned to the AMS, which identifies uniquely an AMS in idle mode with combination with the current Paging Cycle, the current Paging Offset and the current Paging Group ID.
Parent TLV(s)	Paging Information

5.3.2.484 current Paging Group ID

Type	625
Length in octets	6
Value	
Description	Paging Group ID applied to the AMS, which identifies uniquely an AMS in idle mode with combination with the current Paging Cycle, the current Paging Offset and the current Deregistration ID.
Parent TLV(s)	Paging Information

5.3.2.485 Multicarrier capabilities

Type	626
Length in octets	1
Value	LSB 3-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.486 Zone Switch Mode Support

Type	627
Length in octets	1
Value	LSB 1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.487 Capability for supporting A-GPS Method for LBS service

Type	628
Length in octets	1
Value	LSB 1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.488 Interference mitigation supported

Type	629
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16m. 1th ~3rd bit: reserved 4th : DL PMI coordination capability 5th : DL collaborative multi-BS MIMO capability 6th : DL closed-loop multi-BS macro-diversity capability 7th : UL PMI combination capability 8th : Multi_BS sounding calibration capability
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.489 E-MBS capabilities

Type	630
Length in octets	1
Value	LSB 3-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.490 Channel BW and Cyclic prefix

Type	631
Length in octets	2
Value	LSB 15-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.491 frame configuration to support legacy R1.0

Type	632
Length in octets	1
Value	LSB4-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.492 Persistent Allocation support

Type	633
Length in octets	1
Value	LSB1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.493 Group Resource Allocation support

Type	634
Length in octets	1
Value	LSB 1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.494 Co-located coexistence capability support

Type	635
Length in octets	1
Value	LSB 5-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.495 EBB Handover support

Type	636
Length in octets	1
Value	LSB 1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.496 Minimal HO Reentry Interleaving Interval

Type	637
Length in octets	1
Value	LSB 2-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.497 Capability for sounding antenna switching support

Type	638
Length in octets	1
Value	LSB 1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.498 Antenna configuration for sounding antenna switching

Type	639
Length in octets	1
Value	LSB 1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.499 ROHC support

Type	640
Length in octets	1
Value	LSB 1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.500 AMS initiated aGP Service Adaptation Capability

Type	641
Length in octets	1
Value	LSB 1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.501 CS specification for default service flow

Type	642
Length in octets	1
Value	8-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	REG Context

5.3.2.502 SIZE of ICV

Type	643
Length in octets	1
Value	8-bit unsigned integer. 0 = 32 bit-length ICV 1 = 64 bit- length ICV
Description	Size of ICV used for integrity protection in AES-CCM method of Rel.2.0 operation
Parent TLV(s)	Security Negotiation Parameters

5.3.2.503 CAPABILITY_INDEX

Type	644
Length in octets	1
Value	LSB 5-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.504 DEVICE_CLASS

Type	645
Length in octets	1
Value	LSB 5-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.505 CLC Request

Type	646
Length in octets	variable
Value	
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.506 Long TTI for DL

Type	647
Length in octets	1
Value	LSB1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.507 UL sounding

Type	648
Length in octets	1
Value	LSB2-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.508 OL Region

Type	649
Length in octets	1
Value	LSB 3-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.509 DL resource metric for FFR

Type	650
Length in octets	1
Value	LSB1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.510 Max. Number of streams for SU-MIMO in DL MIMO

Type	651
Length in octets	1
Value	3-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.511 Max. Number of streams for MU-MIMO in MS point of view in DL MIMO

Type	652
Length in octets	1
Value	1-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.512 DL MIMO mode

Type	653
Length in octets	1
Value	LSB6-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.513 feedback support for DL

Type	654
Length in octets	2
Value	LSB11-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.514 Subband assignment A-MAP IE support

Type	655
Length in octets	1
Value	LSB1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.515 DL pilot pattern for MU MIMO

Type	656
Length in octets	1
Value	LSB2-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.516 Number of Tx antenna of AMS

Type	657
Length in octets	1
Value	LSB2-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.517 Max. Number of streams for SU-MIMO in UL MIMO(1/2/3/4)

Type	658
Length in octets	1
Value	LSB2-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.518 Max. Number of streams for MU-MIMO in MS point of view in UL MIMO(1/2/3/4)

Type	659
Length in octets	1
Value	LSB2-bit unsigned integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.519 UL pilot pattern for MU MIMO

Type	660
Length in octets	1
Value	LSB3-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.520 UL MIMO mode

Type	661
Length in octets	1
Value	LSB5-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.521 Modulation scheme

Type	662
Length in octets	1
Value	LSB2-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.522 UL HARQ buffering capability

Type	663
Length in octets	1
Value	LSB7-bit integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.523 DL HARQ buffering capability

Type	664
Length in octets	1
Value	LSB7-bit integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.524 AMS DL processing capability per sub-frame

Type	665
Length in octets	1
Value	LSB7-bit integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.525 AMS UL processing capability per sub-frame

Type	666
Length in octets	1
Value	LSB7-bit integer as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.526 FFT size(2048/1024/512)

Type	667
Length in octets	1
Value	LSB3-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.527 Inter-RAT Operation Mode

Type	668
Length in octets	1
Value	LSB2-bit unsigned integer, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.528 Supported Inter-RAT type

Type	669
Length in octets	1
Value	8-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.529 MIH Capability Supported

Type	670
Length in octets	1
Value	LSB1-bit bitmask, as specified in the IEEE802.16m.
Description	This TLV is defined in the IEEE802.16m.
Parent TLV(s)	SBC Context

5.3.2.530 DCR Indication

Type	671
Length in octets	1
Value	01h
Description	An indication that the message containing this TLV was generated as a result of an event related to the AMS either entering or exiting DCR mode
Parent TLV(s)	

5.3.2.531 ARQ SUB BLOCK SIZE

Type	672
Length in octets	1
Value	LSB 3bit unsigned integer as defined in IEEE802.16m.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16m definition.
Parent TLV	ARQ Context

5.3.2.532 MAXIMUM ARQ BUFFER SIZE

Type	673
Length in octets	3
Value	LSB 23bit unsigned integer as defined in IEEE802.16m.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16m definition.
Parent TLV	ARQ Context, REG context

5.3.2.533 MAXIMUM NON ARQ BUFFER SIZE

Type	674
Length in octets	3
Value	LSB 23bit unsigned integer as defined in IEEE802.16m.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16m definition.
Parent TLV	ARQ Context, REG context

5.3.2.534 ARQ ERROR DETECTION TIMEOUT

Type	675
Length in octets	2
Value	16 bit unsigned integer as defined in IEEE802.16m.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16m definition.
Parent TLV	ARQ Context

5.3.2.535 ARQ FEEDBACK POLL RETRY TIMEOUT

Type	676
Length in octets	2
Value	16 bit unsigned integer as defined in IEEE802.16m.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16m definition.
Parent TLV	ARQ Context

5.3.2.536 Host-Configuration-Capability-Indicator

Type	677
Length in octets	1
Value	LSB1-bit bitmask, as specified in the IEEE802.16m..
Description	This TLV is received over the R1 interface and SHALL follow the 802.16m definition.
Parent TLV	ARQ Context

5.3.2.537 Requested-Host-Configurations

Type	678
Length in octets	variable
Value	defined in IEEE802.16m.
Description	This TLV is received over the R1 interface and SHALL follow the 802.16m definition.
Parent TLV	ARQ Context

5.3.2.538 Local Routing Policy

Type	601
Length in octets	1
Value	Enumerator. The values are: - 0x00=no ALR - 0x01=Pre-Authorized ALR - 0x02=Dynamic-Authorized ALR All other values are Reserved.
Description	Used to instruct the ASN to apply for the Local Routing related operation policy for a given service flow.
Parent TLV	SF Info

5.3.2.539 PDFID

Type	679
Length in octets	2
Value	16-bit unsigned integer.
Description	ASN(R6/4) TLV corresponding to the CSN assigned PDFID (section 5.4.3.26 or 5.5.2.25). The value of this attribute derived from the CSN PDFID identifies a packet data flow. A PDFID is used along with the MCBCS Transmission Zone ID in identifying a particular MCBCS flow for a given MCBCS service.
Parent TLV	SF Info

5.3.2.540 Carrier Preassignment Indications

Type	680
Length in octets	1
Value	LSB1-bit bitmask, as specified in the IEEE802.16m.
Description	Indicates whether AMS needs preassignment of secondary carriers at the T-ABS.
Parent TLV	MS Info

5.3.2.541 Carrier Status Indication

Type	681
Length in octets	1
Value	LSB1-bit bitmask, as specified in the IEEE802.16m.
Description	Indicating whether this pre-assigned carrier will be activated immediately after HO procedure is done.
Parent TLV	BS Info

5.3.2.542 Physical carrier index of the secondary carrier index

Type	682
Length in octets	1
Value	LSB6-bit unsigned integer as specified in the IEEE802.16m.
Description	Physical carrier index of the preassigned secondary carrier, which is pair with the Carrier Status Indication TLV.
Parent TLV	BS Info

5.3.2.543 PHY Carrier Index

Type	683
Length in octets	1
Value	LSB6-bit unsigned integer as specified in the IEEE802.16m.
Description	Physical carrier index of ABS.
Parent TLV	BS Info

5.3.2.544 Ranging Initiation Deadline

Type	684
Length in octets	1
Value	LSB8-bit unsigned integer as specified in the IEEE802.16m.
Description	An AMS shall send the AAI-RNG-REQ message during HO until Ranging initiation deadline.
Parent TLV	BS Info

5.3.2.545 Pre-assigned MAPMask Key

Type	685
Length in octets	2
Value	LSB15-bit bitmask, as specified in the IEEE802.16m.
Description	The value of this parameter is the seed used at the T-ABS to initiate the PRBS generator used to scramble the 40-bit A-AMAP IE when the value of the STID included in this message is used as the CRC Mask Masking Code.
Parent TLV	BS Info

5.3.2.546 S-SFH Change Count

Type	686
Length in octets	1
Value	LSB4-bit unsigned integer as specified in the IEEE802.16m.
Description	S-SFH change count of the reference for the included SFH delta information.
Parent TLV	BS Info

5.3.2.547 SA-Preamble Index

Type	687
Length in octets	2
Value	LSB10-bit unsigned integer as specified in the IEEE802.16m.
Description	Indicate the SA-Preamble index of the carrier.
Parent TLV	BS Info

5.3.2.548 S-SFH setting

Type	688
Length in octets	variable
Value	Compound, as specified in IEEE 802.16m, 16.3.5.5.1.2.
Description	This is an IEEE802.16m defined TLV. The S-SFH setting is a TLV value that encapsulates S-SFH subpacket IEs such as SP1, SP2, and SP3 that may be transmitted in the S-SFH.
Parent TLV	RRM BS Info

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.

This specification is based on IETF based RADIUS protocols as specified in RFC2865 [38], RFC2866 [39], and other RADIUS RFCs as referenced in this document. The document reinforces certain RADIUS behaviors and in certain cases extends the protocol defined by the IETF specification. Unless otherwise specified all RADIUS attributes appearing in this specification SHALL be implemented by the receiver of the RADIUS messages. To support extensibility all IETF RADIUS attributes are available to be included in RADIUS messages. Unless otherwise stated, the behavior of the sender and the receiver of the attributes SHALL be compliant to the IETF specification. In particular, the receiver of a RADIUS attribute that are not specified in this document may ignore those attributes that it does not implement by silently discarding the attributes.

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 [53] in an Access-Request during EAP authentication, this attribute provides the appropriate MTU size to avoid exceeding maximum payload size for PKMv2/v3 (2008	0-1[m]	0	0-1[m]	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
		bytes) during EAP exchange (the appropriate fragmentation is assumed in Authentication Server on the EAP application layer). The value of this attribute should be set between 1020 and 2000 bytes (the recommended value is 1400 bytes)." In an Access-Accept the use is as per [38].				
EAP-Message	79	The EAP exchanged transported over RADIUS.	0-n[ac]	1-n	0-n[ac]	0-n[ac]
Message-Authenticator	80	Provides integrity protection for the RADIUS packets as required by [53].	1	1	1	1
WiMAX®-Capability	26/1	Identifies the WiMAX Capabilities supported by the NAS. Indicates capabilities selected by the RADIUS server.	1[ab]	0	1[ab]	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	MAC address of the device (see Section 5.4.3.1).	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 RADIUS Accounting	0-1	0	0-1[a]	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
		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 [52].	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 [53].	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/ABS identifier and usually indicates the location information of the BS/ABS which may be described as Lat/Long/Sector/Carrier information of the serving BS/ABS.	0-1	0	0	0
Mobility-Access-Classifier	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-	26/78	The Proxy Mobile IP	0-1[y]	0	0-1	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Authenticated-Network-Identity		identity allocated by the 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/AMS 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/AMS. 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/AMS 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/AMS. Used only for DHCPv6-based address configuration.	0-1[t]	0	0-1[t]	0
MS-Authenticated	26/90	Indication that MS/AMS has successfully performed device authentication	0	0	0-1	0
Operator-Name	126	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/AMS Certified features relevant for the ASN-GW policy for this MS/AMS.	0	0	0-1[z]	0
Certified-MS-Feature-List-For-BS	26/140	List of MS/AMS Certified features relevant for the BS/ABS policy for this MS/AMS.	0	0	0-1[z]	0

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
Present-Authenticator-Verification-Code	26/141	PA_VC (MSKHash1)	0-1[ad]	0	0	0
OCR-Count	26/142	OCR_COUNT	0-1[ad]	0	0	0
MCBCS-Controller-Server-IPv4	26/106	The IPv4 address of MCBCS Controller/Servers.	0	0	1-n[ae]	0
MCBCS-Controller-Server-FQDN	26/107	The FQDN of MCBCS Controller/Servers	0	0	1-n[ae]	0
MCBCS-Controller-Server-IPv6	26/108	The IPv6 address of MCBCS Controller/Servers.	0	0	1-n[ae]	0
MCBCS-Service-Association-SPI	26/109	MCBCS Service Association Information	0	0	1-n[af]	0
MCBCS-Program-Descriptor	26/110	describes an MCBCS Program	0-1[af]	0	1-n[af]	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 [40]. MSK may be transmitted using MS_MPPE_Send_Key and MS_MPPE_Recv_Key as per [33] 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/AMS. As per [53] 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 IPID 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.

[ab] SHALL be included with service type ‘Framed’. If include with other service-types it SHALL be unchanged for the session from that sent in framed service-type.

[ac] The Access-Request doesn’t include EAP Message if it is used for Authenticator Shifting

The Access-Reject or Access-Accept doesn’t include EAP Messages if it is used for Authenticator Shifting.

[ad] SHALL be included in the Access-Request during the Optimized Combined Relocation or the Optimized Standalone Authenticator Relocation.

[ae] This attribute is only present when the serving ASN supports the MCBCS service.

[af] This attribute is only present when the MS has subscribed to the MCBCS service.

Table 5-6 and Table 5-7 are the Mobility attributes exchanged between the ASN and the HAAA during the Network Access Authentication.

Table 5-6 – 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

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.

Table 5-7 – 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 [66].	0	0	0-1 [a4]	0
vDHCP-RK-Key-ID	26/76	Key identifier associated with the vDHCP-RK, as per [66].	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

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 5-8 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 5-8 – 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[p]	0	1[p]	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

Attribute	TYPE	Description	Access Request	Access Challeng e	Access Accept	Access Reject
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
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	0-1[i]	0	0	0

Attribute	TYPE	Description	Access Request	Access Challeng e	Access Accept	Access Reject
		Address field in the BU.				
Acct-Interim-Interval	85	Indicates the number of seconds between each interim update in seconds for this specific session.	0	0	0-1	0
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

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.

[p] SHALL be included with service type ‘Framed’. If include with other service-types it SHALL be unchanged for the session from that sent in framed service-type.

Table 5-9 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 5-9 – 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	1	0	1	0

Attribute	TYPE	Description	Access Request	Access Challeng e	Access Accept	Access Reject
		the RADIUS server.				
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®-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
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

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 5-10 defines the RADIUS messages that are exchanged between a DHCP server and the HAAA.

Table 5-10 – 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

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
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 5-11 describes the RADIUS attributes sent from the HAAA to the Hot-Line Device (NAS or the HA).

Table 5-11 – 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 [38] SHALL NOT be include in the RADIUS packet. A RADIUS packet that violates this rule SHALL be discarded.

Table 5-17 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 [52] are supported with the additional information as specified by this table.

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 [41]).

5.4.1.6 Offline Accounting

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. • 0x00 = Uncompressed counts • 0x01 = Compressed counts	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]
Local-Routing-Indication	26/244	Indicates whether the flow is local routing enabled by ASN-GW, at any point during the accounting period.	0-1[8]	0-1[8]	0-1[8]

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.

[8] If included, two sets of L3 accounting counters may be contained in a given stop and interim Accounting message where the first one is generated in the ASN for normal traffic and the second one is generated in the ASN for local-routed traffic. If only one set of L3 Counters is present, it is for the normal traffic by default. I.e. Normal traffic counters are present even if there are only local routed traffic.

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/AMS 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/AMS 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/AMS. 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/AMS by VCSN. This identifies the IP-Session.	0-1[5]	0-1[5]	0-1[5]
Visited-Framed-IPv6-	26/80	The IPv6 prefix assigned to the MS/AMS by	0-1[5]	0-1[5]	0-1[5]

Name	Type	Description	Start	Int	Stop
Prefix		VCSN. This identifies the IP Session.			
Visited-Framed-Interface-Id	26/81	The IPv6 interface id assigned by the visited CSN to be used for the MS/AMS. 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 scenarios.	0-1 [1,4] [6,7]	0-1 [1,4] [6,7]	0-1 [1,4] [6,7]
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]

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;

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	MAC address of the device (see Section 5.4.3.1).	0-1[2]	0-1[2]	0-1[2]

Notes:

[1] SHALL be included if received in an RADIUS Access-Accept packet.

[2] SHALL be included from messages coming from a NAS. SHALL NOT be included from messaged coming from an HA.

5.4.1.6.4 Infrastructure Identifiers

Name	Type	Description	Start	Int	Stop
NAS-ID	32	The identifiers of the NAS generating this record.	0-1[1]	0-1[1]	0-1[1]
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	126	The WRI-Code of the VNSP and HNSP.	0-2[5]	0-2[5]	0-2[5]

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	0-2[2][3]	0-2[2][3]
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	0-2[3]	0-2[3]
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	0-2[2][3]	0-2[2][3]
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	02[3]	0-2[3]
Acct- Input -Gigawords	52	Incremented when attribute 42 overflows.	0	0-2[2][3]	0-2[2][3]
Acct- Output -Gigawords	53	Incremented when attribute 43 overflows.	0	0-2[3]	0-2[3]
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]

Name	Type	Description	Start	Int	Stop
Control-Packets-Out	26/33	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]
Control-Octets-Out	26/34	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.	0	0-1[1]	0-1[1]
Acct- Input -Packets-Gigaword	26/48	Incremented when attribute 47 overflows.	0	0-2[2][3]	0-2[2][3]
Acct- Output -Packets-Gigaword	26/49	Incremented when attribute 48 overflows.	0	0-2[3]	0-2[3]

1 **Notes:**

[1] SHALL NOT be reported by a HA.

[2] SHALL Not be reported in MCBCS case

[3] If the given VSA is present twice, it indicates the first one is for the normal traffic, and the second one is for the local-routed traffic. If present once, it is always for the normal traffic.

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/AMS'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.

5.4.1.6.8 Granted-QoS

Name	Type	Description	Start	Int	Stop
Uplink-Granted-QoS	26/30	Uplink QoS granted to the MS/AMS.	0	0-1 [1][2]	0-1 [1][2]
Downlink-Granted-QoS	26/63	Downlink QoS granted to the MS/AMS.	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 [52] with the following:

Attribute	TYPE	Description	DR	DR-ACK	DR-NAK
User-Name	1	The NAI of the MS/AMS as received during Access-Authentication.	1	0	0
Calling-Station-Id	31	The Calling Station Id (MAC address of device) as received during access authentication (see Section 5.4.3.1). The format of the Calling Station Id SHALL be the same as the last value received from the NAS to which this message is being sent.	1[b]	0	0
WiMAX®-Session-Id	26/4	A unique per realm identifier assigned to the WiMAX session by the hAAA during network	1	0	0

Attribute	TYPE	Description	DR	DR-ACK	DR-NAK
		entry.			
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/ABS sends the RES-CMD/AAI-RES-CMD to the MS/AMS.	0-1	0	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.	0-1[a]	0	0
NAS-IP-Address	4	NAS IP address.	0-1[a]	0	0
NAS-IPv6-Address	95	NAS-IPv6 address.	0-1[a]	0	0

[a] NAS-Identifier SHALL appear in the Disconnect-Request Message if vAAA or AAA proxy are available in the path to reach NAS. One of NAS-IP-Address or NAS-IPv6 address MAY also appear in similar case.

[b] The format of the Calling Station ID SHALL be the same as the last value received from the NAS to which this message is being sent.

RADIUS Disconnect-ACK message is sent without any additional parameters

5.4.1.7.1 RADIUS Disconnect NACK Message

Table 5-12 – RADIUS Disconnect NACK Message

Attribute	ID	AR	Description	Source
Error-Cause	101	1		RFC5176

5.4.1.8 RADIUS Change of Authorization Messages

RADIUS Change of Authorization as specified in [52] are available to be sent between the HAAA server and ASN-GW or HA/LMA to modify an existing session. Modifications are possible by sending new values of existing attributes or sending new attributes.

This section defines the use of the attributes contained in the Change of Authorization message and Change of Authorization Ack/NACK messages.

The NAS SHALL respond back with a change of authorization ACK or NACK message as per [52].

RADIUS COA messages require identification attributes as per [52]. The following table list the identification attributes to be used in the context of WiMAX. Some of these attributes are defined by [52] but their use is describe in the WiMAX context. Some of these attributes are WiMAX specific. As per [52] attributes used for session identification (NAS Identifiers and User Session Identifiers) must not be used to change session parameters.

Table 5-13 – Integrity-Protection

Attribute	ID	AR	Description
Message-Authenticator	80	1	Provides integrity protection for the RADIUS packets as required by [52]

Table 5-14 – NAS Identifiers

Attribute	ID	AR	Description
NAS-Identifier	32	1	FQDN of the NAS currently hosting the session.
NAS-IP-Address	4	0-1	IPv4 address of the NAS hosting the session.
NAS-IPv6-Address	95	0-1	IPv6 address of the NAS hosting the session.

Table 5-15 – User Session Identifiers

Attribute	ID	AR	Description
User-Name	1	1	User-Name of the session. The NAI must contain only the identity of the user used during network entry without any of the WiMAX decoration "{}" or routing decoration and the realm if received. The realm is used for the reverse path check described in [52]
WiMAX-Session-Id	26/4	1	Identifies the WiMAX session.
Calling-Station-Id	31	1	The Calling Station Id (MAC address of device) as received during access authentication (see Section 5.4.3.1). The format of the Calling Station ID SHALL be the same as the last value received from the NAS to which this message is being sent.
Chargeable User Identity	89	0-1	If present in the Access-Request it must be included in the COA. This attribute identifies the user session associated with the COA message.
Framed-IP-Address	8	0-1	If present identifies the IPv4 session to be modified. In certain cases, the COA is applicable to a specific IPv4 session. In these cases, this attribute identifies the IPv4 session.

Attribute	ID	AR	Description
Framed-Interface-Id	96	0-1	If present identifies the IPv6 session to be modified. In certain cases, the COA is applicable to a specific IPv6 session. In these cases, this attribute identifies the IPv6 session.
Framed-IPv6-Prefix	97	0-1	If present identifies the IPv6 session to be modified. In certain cases, the COA is applicable to a specific IPv6 session. In these cases, this attribute identifies the IPv6 session.
Acct-Session-Id	44	0-1	SHOULD NOT be used.
Acct-Multi-Session-Id	87	0-1	SHOULD NOT be used. But if used it shall contain the same value as WiMAX-Session-Id attribute.

Other attributes as specified by [52] may also be included to identify the session.

The rest of the attribute that appear in the COA are the attributes that are the new authorization attributes that modify the session respectively specific IP-session (as identified by the presence of IP session attributes) or deal with MCBCS specific parameters. The attributes available to be used are defined in the RFCs and the WiMAX specific attributes as defined in this document. These include the Hotlining attribute defined above or the PCC

Table 5-16 – RADIUS COA attributes between NAS and HAAA for Flow modification

Attribute	TYPE	Description	COA	COA-ACK	COA-NAK
Packet-Flow-Descriptor	26/28	The pre-provisioned Service Flows	0[c]	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,b]	0	0
MCBCS-Program-Descriptor	26/110	Identify the MCBCS Program	1-n[d]	1-n[d]	0
R3-Multicast-IP-address	26/246	Identify the content multicast IP address which user subscribed for	1[d]	0	0
MCBCS-Controller-Server-IPv4	26/106	MCBCS Controller/Server IPv4 Address	1[d]	0	0
MCBCS-Controller-Server-IPv6	26/108	MCBCS Controller/Server IPv6 address	1[d]	0	0
MCBCS-Controller-Server-FQDN	26/107	MCBCS Controller/Server FQDN	1[d]	0	0
MCBCS-Service-Association-SPI	26/109	MCBCS Service Association Information	0-1[e]	0	0

Notes:

[a] Conditional mandatory: see requirements for Packet-Flow-Descriptor.

[b] 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.

[c] Support of Packet-Flow-Descriptor is deprecated in this release. Packet-Flow-Descriptor-V2 SHALL only be used instead.

[d] This parameter SHALL be included for the case of MCBCS flow only.

[e] This parameter may be included for the case of an MCBCS flow.

Table 5-17 – RADIUS COA (from HAAA to HLD) for Hotling

Attribute	TYPE	Description	COA	COA-ACK	COA-NAK
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

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 [38] SHALL NOT be include in the RADIUS packet. A RADIUS packet that violates this rule SHALL be discarded.

Table 5-18 – RADIUS COA attributes between NAS and HAAA for ASN Local Routing

Attribute	TYPE	Description	COA	COA-ACK	COA-NAK
ALR-Command	26/245	Carries the dynamic ALR request/response.	1	1	0

5.4.1.9 RADIUS Messages for ASN Local Routing

Table 5 X shows the RADIUS attributes exchanged between the NAS and the HAAA for dynamically authorizing ASN local routing.

Table 5-19 – RADIUS Messages between NAS and HAAA for ALR

Attribute	TYPE	Description	Access Request	Access Chall.	Access Accept	Access Reject
ALR-Command	26/245	Carries the dynamic ALR request/response.	1	0	1	0

5.4.2 Standard RADIUS Attributes

This section describes WiMAX-specific details regarding the use of standard RADIUS attributes. Unless otherwise specified in this section, use of any standard RADIUS attribute SHALL comply with the stated behavior in its respective RFC/draft.

5.4.2.1 Calling-Station-Id

In various RADIUS messages the Calling-Station-Id Attribute (Type 31 in RFC 2865 [38]) is used to carry the MAC address of the device. The MAC address can be encoded in one of two ways: As a 6-byte binary value, or as a 17-byte upper case ASCII value as defined by RFC 3580 [83] sec 3.21 and 802-2001 in canonical order. For example, "00-10-A4-23-19-C0" is a valid ASCII-formatted MAC address, whereas 00-10-a4-23-19-c0 and 00:10:A4:23:19:C0 are not valid. RADIUS client SHALL support at least one of these formats, and MAY support both. RADIUS server SHALL support both formats. In the case the RADIUS Client supports both formats it SHALL select one of them and SHALL use it for the remainder of the WiMAX session. When including the Calling-Station-Id in a message to the RADIUS Client, the RADIUS server SHALL use the same format as was last received from that RADIUS Client (as determined by the NAS-Identifier).. Receiver of a RADIUS message can determine the format of the MAC address by inspecting the length of the attribute: 6 byte data means that the MAC address is formatted in binary, and 17 byte means as ASCII. Note that different RADIUS clients may use different formats. Therefore, the same RADIUS server may be subject to using different formats for the same MS session across handovers.

5.4.3 WiMAX® RADIUS VSAs Definitions

WiMAX® RADIUS VSAs are transported in a RADIUS Vendor Specific Attribute.

The following describes the general format of WiMAX VSAs.

```
    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)           |             String
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type	26 for Vendor-Specific.
Length	Length of the entire structure which is given by: The length of the Header (=6) plus the length of the WiMAX Vendor Attribute.
Vendor-Id	The SMI Network Management Private Enterprise Code of the Vendor in network byte

	order, as defined in the "Assigned Numbers" [57]. The Vendor-Id for WiMAX is 24757.
String	Contains one WiMAX Vendor attribute which is formatted as specified below.

```
  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

 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |   WiMAX Type  |  Length       |  Continuation |    Value
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WiMAX® Type	0 is reserved. 1-254 WiMAX Types as defined below. 255 is reserved.
Length	>= 3. Length of the WiMAX attribute including the WiMAX Type, length, Continuation and Value field.

Continuation	The Continuation Field is defined as follows:
	` 0`
	` 0 1 2 3 4 5 6 7`
	`+-+-+-+-+-+-+-+-+`
	`|C|r|r|r|r|r|r|r|`
	`+-+-+-+-+-+-+-+-+`
	The C-bit of the continuation field indicates if a WiMAX attribute is being fragmented.
	When the C-bit is set to one '1' this indicates that the attribute is being fragmented that is the next WiMAX VSA of the same WiMAX type is to be appended to this attribute.
	When the C-bit is set to zero '0' this indicates that the next attribute is not a fragment of this attribute.
	A WiMAX attribute that is not being fragmented 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.
	The r-bits are reserved for future use. They SHALL be set to zero by the sender and SHALL be ignored by the receiver.

Value	Value of the attribute which is one of the attribute formats given below or one or more sub-TLVs.

A sub-TLV has the following format:

```
  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

 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | SUB-TYPE      |  Length       |  Value
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	0 is reserved 1-254 WiMAX Sub-Types 255 is reserved
Length:	>= 3. Length of the WiMAX Sub-attribute including the Sub-type (1 octet), and Length Field (1 octet) and the length of the Value field (1 octet).

Value	Value of the attribute which is of one of the attribute formats defined below.

For each WiMAX VSA that consists of sub-TLVs a table summarizing the size and the presence of the TLVS in each RADIUS message is given. The table indicates whether the sub-TLV is required or not in each message and how many occurrences of the sub-TLV may appear in the message as follows:

0	The sub-TLV SHALL NOT appear.
1	The sub-TLV SHALL appear.
0-1	The sub-TLV MAY appear only once.
0-n	The sub-TLV MAY appear more than once.
1-n	The sub-TLV SHALL appear at least once.

The abbreviations used for the column headings for these tables are:

AR	Access-Request or if the attribute also appears in accounting then Accounting Request.
AA	Access-Accept.
AC	Access-Challenge.
R	Access-Reject.

The following table lists the attribute formats used in describing the WiMAX VSAs.

Attribute Format	Length	Description
Unsigned-Byte	1 octets	0 to 2^8-1. Most significant bit first.
Unsigned-Short	2 octets	0 to 2^{16}-1. Most significant bit first.
Unsigned Integer	4 octets	0 to 2^{32}-1. Most significant bit first.
Text	> 1 octet	Contains UTF-8 encoded 10646 [7] characters. Text of length zero (0) SHALL NOT be sent; omit the entire attribute instead.
Octet-String	> 1 octet	Contains binary data (values 0 through 255 decimal, inclusive). Strings of length zero (0) SHALL NOT be sent; omit the entire attribute instead.
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 otherwised 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.

```
 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 |7|6|5|4|3|2|1|0|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

5.4.3.1 WiMAX®-Capability

```
 0                   1                   2                   3

 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |  Length       |            Vendor-Id          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Vendor-Id (cont)           | WiMAX TYPE    |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Continuation |            TLVs
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	1 for WiMAX-Capability Attribute
Description	In an Access-Request the attribute identifies the WiMAX-Capabilities supported by the ASN or the HA. In an Access-Accept, identifies the options selected by the RADIUS server.
Length	6 + 3 + TLVs
Continuation	C-bit = 0
Value	One or more of the following sub-TLVs

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
14	ASN PCC Capabilities	2+1	0-1[l][k]	0-1[m][k]	0	0
15	Packet-Flow-Operation-Policy	2+1	0-1[n]	0	0	0
16	Local-Routing-Support	2+1	0-1[m]	0	0	0

1 **Notes:**

[a] The absence of this sub-TLV in an Access-Request (AR) means that the HA does not support Hot-Lining. An ASN-GW MUST always include the Hotlining-Capability TLV.

[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.

[l] The absence of this sub-TLV in an Access-Request (AR) means that the ASN does not support PCC.

[m] The absence of this sub-TLV in an Access-Accept (AA) message means that the hCSN does not request to activate PCC Framework in ASN for the MS.

[n] The absence of this sub-TLV in an Access-Request (AR) implies that the serving ASN does not support Packet-Flow-Operation-Policy. Packet flow operation policies are applied based on local policies.

[m] The absence of this sub-TLV in an Access-Request (AR) implies that the ASN does not support SF-based Local Routing.

2

TLV ID	1 for WiMAX-Release
Description	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.
Length	2+Length of string
Value	A string indicating a WiMAX Release. Valid values are "1.0", “1.5” or "1.6".

TLV ID	2 for Accounting-Capabilities
Description	In an Access-Request describes the accounting capabilities that are supported by the sender (ASN or HA). In an Access-Accept, describes the accounting capabilities that the server selected for the session.
Length	2+1 octet
Value	In an Access-Request the NAS (ASN, HA) specifies the accounting capabilities that it supports as a bit-map. In an Access-Accept the server 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. • Bit #0 = IP/ETH-Session-based accounting. Default value for the ASN. • Bit #1 = Flow-based accounting for IP-CS. • Bit #2 = Flow-based accounting for ETH-CS. • Bit #3 = R3-OC based accounting • Bit#4 = R3-OFC based offline accounting 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. All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

TLV ID	3 for Hotlining-Capabilities
Description	In an Access-Request describes the hotline capacities supported by the ASN or the HA.
Length	2+1 octet
Value	In an Access-Request the NAS or HA specifies the 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. • Bit #0 = Profile-based Hot-Lining is supported (using the Hotline-Profile-ID VSA). • Bit #1 = Rule-based Hot-Lining is supported using NAS-Filter-Rule. • Bit #2 = Hot-Lining HTTP Redirection is supported. • Bit #3 = Rule-based Hot-Lining is supported using IP-Redirection rule. Bit#1 and Bit#2 MUST SHALL be set as a minimum by the ASN-GW. All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

1

TLV ID	4 for Idle-Mode-Notification-Capabilities
Description	In an Access-Request or Accept-Accept describes the idle mode notification capabilities supported by the ASN or required by the CSN. Omission of this sub TLV means that Idle Mode Notification is not supported or required.
Length	2+1 octet
Value	In an Access-Request the NAS (ASN) specifies if idle mode notification is supported at the ASN. In Access-Accept the HAAA specifies if idle mode notification is required at the HAAA. • 0x00 = Idle Mode notification is not supported or is not required. • 0x01 = Idle Mode notification is supported or is required.

2

TLV ID	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.)
Description	
Length	
Value	

3

TLV ID	6 for Authorized-Network-Services
Description	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. Note: A NAS that supports this attribute MAY treat the information as a hint as to the mobility capabilities of the MS rather then an authorization for the use of mobility services.
Length	2+4 octet
Value	4 octet Bit Mask with the following values: • Bit #0 – CMIP4 • Bit #1 – PMIP4 • Bit #2 – Simple IPv4 • Bit #3 – CMIP6 • Bit #4 – PMIP6 • Bit #5 – Simple IPv6

	• Bit #6 – Simple ETH Service • Bit #7 – MIP based ETH Service • Bit #8 – L2 DHCP Relay[a] The rest of the bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

[a] L2 DHCP Relay can be selected with either Simple Ethernet Service or MIP based Ethernet Service.

TLV ID	7 for ASN-Network-Service-Capabilities
Description	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
Length	2+4 octet
Value	4 octet Bit Mask with the following values: • Bit #0 – DHCPv4 Relay • Bit #1 – DHCPv6 Relay • Bit #2 – DHCPv4 Proxy • Bit #3 – DHCPv6 Proxy • Bit #4 – CMIPv4 FA • Bit #5 – PMIPv4 FA and Client • Bit #6 – AR with IPv4 Transport[39] • Bit #7 – AR with IPv6 Transport[40] • Bit #8 – L2FW • Bit #9 – ETH Service FA • Bit #10 – L2 DHCP Relay • Bit #11 – MAG All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

TLV ID	8 for VCSN-Network-Service-Capabilities
Description	This TLV is included in a RADIUS Access-Request packet to the RADIUS server and indicates VCSN related Network Service Capabilities
Length	2+4 octet
Value	4 octet Bit Mask with the following values: • Bit #0 – DHCPv4 Server • Bit #1 – DHCPv6 Server • Bit #2 – HAv4

[39] AR with IPv4 transport indicates the support of Simple IP service using IPv4 transport

[40] AR with IPv6 transport indicates the support of Simple IP service using IPv6 transport

	• Bit #3 – HAv6 • Bit #4 – eCB • Bit #5 – ETH HA • Bit #6 – LMA All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

TLV ID	9 for Visited-Authorized-Network-Services
Description	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.
Length	2+4 octet
Value	4 octet Bit Mask with the following values: • Bit #0 – CMIP4 • Bit #1 – PMIP4 • Bit #2 – Simple IPv4 • Bit #3 – CMIP6 • Bit #4 – PMIP6 • Bit #5 – Simple IPv6 • Bit #6 – Simple ETH Service • Bit #7 – MIP based ETH Service • Bit #8 – L2 DHCP Relay[a] All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

[a] L2 DHCP Relay can be selected with either Simple ETH Service or MIP based ETH Service

TLV ID	10 for Mobility-Access-Capabilities
Description	In an Access-Request describes mobility access supported by the ASN.
Length	2+1 octet
Value	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. • Bit#0 = Fixed/Nomadic access is not supported. Only Mobility. • Bit#1 = Fixed/Nomadic access is supported alongside Mobility. • Bit#2 = Only Fixed/Nomadic access is supported. No Mobility. All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

TLV ID	11 for ROHC-Support
Description	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.
Length	2+1 octet
Value	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. • Bit #0 = ROHC capability is supported or is required. All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

TLV ID	12 for Release-Supported
Description	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.
Length	2+length of string
Value	String of supported releases separated by commas ‘,’. The list is ordered from the lowest version to the highest version supported.

TLV ID	13 for Version-Negotiation-Flag
Description	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.
Length	2+1 octet
Value	One octet enumeration with the following value: [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. [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. [3] Set by the HAAA to indicate that the Access-Challenge is for version negotiation only. All other values are reserved.

TLV ID	14 for ASN PCC Capabilities
Description	In the initial Access-Request, it advertises the ASN network capabilities to support PCC Framework. If included in an Access Accept, it presents hCSN request to activate PCC Framework in ASN for the MS (IP-CAN session establishment by A-PCEF).
Length	2+1 octet
Value	Reserved. Must be set to 0.

TLV ID	15 for Packet-Flow-Operation-Policy
Description	This TLV MAY be included in an Access-Request (AR) message by the NAS.
Length	2+1 octet
Value	One octet bitmap field with the following values: Bit-0 – reserved for per SF airlink encryption on/off capability indicator. When set to “0”, the serving ASN does not support per SF airlink encryption on/off capability. When set to “1” the serving ASN supports per SF airlink encyrption on/off capability. All other bits are reserved. The sender shall clear the reserved bits to zero and the receiver shall ignore the reserved bits.

TLV ID	16 for Local-Routing-Support
Description	This TLV MAY be included in an Access-Request (AR) message by the NAS.
Length	2+1 octet
Value	Bitmap. The values are: - Bit #0 – SF-based Local Routing at ASN-GW All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits

5.4.3.2 Void

5.4.3.3 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                |
+-+-+-+-+-+-+-+-+
```

WType-ID	3 for GMT-Timezone-offset
Description	The current offset in seconds of the local time at the NAS with respect to GMT time.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	4 Octet-String interpreted as a Signed Integer (Most significant bit first) indicating a timeoffset in seconds.

5.4.3.4 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	4 for WiMAX-Session-Id
Description	A unique per realm identifier assigned to the WiMAX session by the hAAA during network entry. The NAI contained in the User-Name and the WiMAX-Session-Id forms a unique identifier of the session at the NAS. The same value is included in all subsequent AAA transactions packets for that WiMAX 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.
Length	6 + 3 + Length of ID
Continuation	C-bit = 0
Value	Octet String. The value of the WiMAX-Session-Id.

5.4.3.5 MSK

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |  Length       |            Vendor-Id          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Continuation |  SALT                         |   String
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	5 for MSK
Description	The Master Session Key determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted MSK.
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2 octet SALT (see [40]) and String containing the encrypted MSK formulated as per [40].

5.4.3.6 hHA-IP-MIP4

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |  Length       |            Vendor-Id          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Continuation |   HA-IP
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	6 for hHA-IP-MIP4
Description	The IPv4 address of the h-HA for MIP4v4.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing an IPv4 address (most significant bit first).

5.4.3.7 hHA-IP-MIP6

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Continuation |   HA-IP
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	7 for hHA-IP-MIP6
Description	The IPv6 address of the h-HA used for MIPv6.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet string containing an IPv6 address (most significant bit first).

5.4.3.8 hDHCPv4-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   |   DHCP-Server IPv4
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	8 for hDHCPv4-Server
Description	The IPv4 address of the home DHCP-Server to use for IPv4 address allocation by the ASN.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing an IPv4 address (most significant bit first).

5.4.3.9 hDHCPv6-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   |   DHCP-Server  IPv6
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	9 for hDHCPv6-Server
Description	The IPv6 address of the home DHCP-Server to use for IPv6 allocation by the ASN.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet string containing an IPv6 address (most significant bit first).

5.4.3.10 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	10 for MN-hHA-MIP4-KEY
Description	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.
Length	6 + 3 +2(SALT)+ Length of the encrypted MN-hHA-MIP4-KEY
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2 octet SALT (see [40]) and String containing the encrypted MN-hHA-MIP4-KEY formulated as per [40].

5.4.3.11 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                              |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |               |
   +-+-+-+-+-+-+-+-+
```

WType-ID	11 MN-hHA-MIP4-SPI
Description	The SPI associated with the MN-HA-MIP4-KEY.
Length	6+3+4
Continuation	C-bit = 0
Value	Unsigned 32-bit Integer. In an Access-Accept sent from the home AAA to the ASN the value is set to SPI-PMIP4.

5.4.3.12 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	12 for MN-hHA-MIP6-KEY
Description	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.
Length	6 + 3 + 2(SALT)+ Length of the encrypted MN-hHA-MIP6-KEY
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2 octet SALT (see [40]) and String containing the encrypted MN-hHA-MIP6-KEY formulated as per [40].

5.4.3.13 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                              |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                |
+-+-+-+-+-+-+-+-+
```

WType-ID	13 MN-hHA-MIP6-SPI
Description	The SPI associated with the MN-hHA-MIP6-KEY/
Length	6 +3+4
Continuation	C-bit = 0

Value	Unsigned 32-bit Integer.

5.4.3.14 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	14 for FA-RK-KEY
Description	The FA-RK determined during EAP authentication by the RADIUS server and passed to the NAS upon successful EAP authentication. It is used by the NAS to generate MN-FA keys.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted FA-RK-KEY.
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2-octet SALT (see [40]) and String containing the encrypted FA-RK formulated as per [40].

5.4.3.15 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	15 for hHA-RK-KEY
Description	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.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted hHA-RK-KEY.
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2-octet SALT (see [40]) and String containing the encrypted HA-RK

	formulated as per [40].

5.4.3.16 hHA-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  |     TLV
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	16 for hHA-RK-SPI
Description	The SPI used for the hHA-RK.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

5.4.3.17 hHA-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  |     TLV
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	17 for hHA-RK-Lifetime
Description	The Lifetime of the hHA-RK and derived keys.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first representing the time before the key expires in seconds.

5.4.3.18 RRQ-HA-IP

```
    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  |    RRQ HA-IP
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	18 for RRQ-HA-IP
Description	The IPv4 or IPv6 address of the HA as contained in the MIP Registration Request or the BU.
Length	6 + 3 + (4 for IPv4 or 16 for IPv6)
Continuation	C-bit = 0
Value	Octet string containing an IPv4 or IPv6 address (most significant bit first).

5.4.3.19 RRQ-MN-HA-KEY

```
   0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  | Continuation  |    SALT                       |     String
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	19 for RRQ-MN-HA-KEY
Description	The MN_HA key sent by the HAAA to the HA to be used to validate the MN-HA-AE of the Mobile IP Registration Request.
Length	6 + 3 +2(SALT)+ Length of the encrypted RRQ-MN-HA-KEY
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2-octet SALT (see [40]) and String containing the encrypted RRQ-MN-HA-KEY formulated as per [40].

5.4.3.20 Time-Of-Day-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  |     TLV
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	20 for Time-Of-Day-Time
Description	The attribute identifies the time in a day at which a tariff switch occurs for volume-based billing and duration-based billing.
Length	6 + 3 + Length of Sub TLVs
Continuation	C-bit = 0

Value	The following sub-TLVs

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	Hour	3	0	1	0	0
2	Minute	3	0	1	0	0
3	UTC Offset	6	0	1	0	0

TLV ID	1 for Hour
Description	Specifies the hour of the day in 24-hour format for the tariff change.
Length	2+1 octet
Value	0-23

TLV ID	2 for Minute
Description	Specifies the minute of the hour for the tariff change.
Length	2+1 octet
Value	0-59

TLV ID	3 for UTC Offset
Description	Specifies the time zone offset from UTC for the tariff change in seconds.
Length	2+4 octets
Value	

5.4.3.21 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |
+-+-+-+-+-+-+-+-+
```

WType-ID	21 for Session-Continue
Description	This attribute when set to 'true' means it is not the end of a Session and an Accounting Stop is immediately followed by an Account Start Record. 'False' means end of a session.
Length	6 + 3 + 4

Continuation	C-bit = 0
Value	If the value is set to 1 session continue is true. If the value is set to 0 session continue is false.

5.4.3.22 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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	22 for Beginning-of-Session
Description	This attribute when set to 'true' means that this Accounting Start packet marks the start of a new flow. If set to 'False', this Accounting Start message is a continuation of a previous flow.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	If the value is set to 1 Beginning-of-Session is true. If the value is set to 0 Beginning-of-Session is false.

5.4.3.23 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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |               |
 +-+-+-+-+-+-+-+-+
```

WType-ID	23 for Network-Technology
Description	This attribute indicates which type of WiMAX session is being used.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer. The enumeration is defined as follows: • 0 = Simple IPv4 • 1 = Simple IPv6 • 2 = PMIP4 • 3 = CMIP4

	• 4 = CMIP6 • 5 = void • 6 = Simple ETH • 7 = MIP based ETH • 8 = PMIP6 • 9 - 2^{32}-1 = Reserved

5.4.3.24 Hotline-Indication

```
    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  |          Hotline Indication String
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	24 for Hotline-Indication
Description	This attribute in a RADIUS Accounting-Request message indicates to back-office systems (billing audit systems) that the session has been Hot-Lined. Exactly one Hot-Line Accounting Indication VSA may appear in a RADIUS Access-Accept packet or RADIUS COA message. If the Hot-lining Device (ÁSN-GW, HA/LMA) received this attribute in a RADIUS Access-Accept or COA message, then it SHALL include the attribute in any subsequent RADIUS Accounting messages for that session.
Length	6 + 3 + Length of String (>0).
Continuation	C-bit = 0
Value	A string value which is to be opaque.

5.4.3.25 Prepaid-Indicator

```
    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  | Flag          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	25 for Prepaid-Indicator
Description	This attribute appears in Accounting messages and indicates to the backoffice that this session was associated with a prepaid user (on-line accounting). If the attribute is not present the session is deemed to be an offline (not prepaid) session.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Unsigned Octet. An enumerated value set to 1 indicates the session is an online session. A

	value of ‘0’ indicates offline session.

5.4.3.26 PDFID

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |  Length       |           Vendor-Id           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |     Unsigned Short            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	26 for PDFID
Description	This value of this attribute matches all records from the same packet data flow. PDFID is assigned by the CSN and remains constant through all handover scenarios. A PDFID can represent a unidirectional flow or a bi-directional flow. A PD-flow is bound to a single WiMAX service flow when PDFID represents a unidirectional flow; and two service flows when PDFID represents a bi-directional flow.
Length	6 + 3 + 2
Continuation	C-bit = 0
Value	Unsigned Short. Packet Data Flow Identifier. (Most significant bit first)

5.4.3.27 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |  Length       |           Vendor-Id           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |    Unsigned Short             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	27 for SDFID
Description	The value of this attribute matches all packet data flows from the same service data flow. SDFID is assigned by the CSN and remains constant through all handover scenarios.
Length	6 + 3 + 2
Continuation	C-bit = 0
Value	Unsigned Short. Service Data Flow Identifier (Most significant bit first).

5.4.3.28 Packet-Flow Descriptor (This Attribute is deprecated in this release)[41]

5.4.3.29 QoS-Descriptor

```
   0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  Continuation |               TLVs
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type-ID	29 for QoS-Descriptor
Description	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.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types are described below.

Table 5-20 – QoS-Descriptor attribute presence

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

[41] This Attribute SHALL not be used, as the support of Packet Flow Descriptor is depricated in this release. Only Packet Flow Descriptor V2 SHALL be supported instead.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR	COA	COA-ACK	COA-NAK
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
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
19	Priority-Indication	1	0	0-1[e]	0	0	0-1[e]	0	0

Notes:

[a] The inclusion of these attributes is as per the value of the Schedule-Type in accordance to Table 5-19.

[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 MCBCS Service.

[e] This attribute shall be present for ETS support.

Table 5-21 – 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

ID	QoS Parameter	BE	ERT-VR	UGS	RT-VR	NRT-VR
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]

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.

TLV ID	1 for QoS ID
Description	A unique ID for this QoS specification in this packet. The ID is used in the Service-Flow-Descriptor attribute to reference a specific QoS Spec (see the UplinkQoSID and DownlinkQoSID TLVs).
Length	2+1
Value	Unsigned Octet representing an ID.

TLV ID	2 for Global Service Class Name
Description	This parameter represents the Global Service Class Name as defined in IEEE802.16e.
Length	2+6
Value	String of length 6 octet containing the name of the global service class name. Values are defined in IEEE802.16e.

TLV ID	3 for Service Class Name
Description	This parameter represents the Service Class Name as defined in IEEE802.16e.
Length	2+Length of Service Class String (>=1)
Value	String containing the name of the service class name. Values are defined in IEEE802.16e.

TLV ID	4 for Schedule Type
Description	The parameter specifies the Uplink Granted Scheduling Type as defined in IEEE802.16e.
Length	2+1
Value	Octet enumeration with the following values defined: • 0 = Reserved • 1 = Reserved

	• 2 = Best Effort • 3 = nrtPS • 4 = rtPS • 5 = Extended rtPS • 6 = UGS • 7 – 255 = Reserved

TLV ID	5 for Traffic Priority
Description	The value of this parameter specifies the priority assigned to a service flow. Given two service flows identical in all QoS parameters besides priority, the higher priority service flow should be given lower delay and higher buffering preference. For otherwise non-identical service flows, the priority parameter should not take precedence over any conflicting service flow QoS parameter. The specific algorithm for enforcing this parameter is not mandated here.
Length	2+1
Value	0 to 7 – Higher numbers indicate higher priority. Default 0.

TLV ID	6 for Maximum Sustained Traffic Rate
Description	This parameter defines the peak information rate of the service. The rate is expressed in bits per second and pertains to the SDUs at the input to the system. Explicitly, this parameter does not include MAC overhead such as MAC headers or CRCs. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. If this parameter is omitted or set to zero, then there is no explicitly mandated maximum rate. This field specifies only a bound, not a guarantee that the rate is available. The algorithm for policing to this parameter is left to vendor differentiation and is outside the scope of the standard.
Length	2+4
Value	Unsigned Integer specifying a rate in bits per second.

TLV ID	7 for Minimum Reserved Traffic Rate
Description	Represents the Minimum Reserved Traffic Rate as defined in IEEE802.16e. This parameter specifies the minimum rate reserved for this service flow. The rate is expressed in bits per second and specifies the minimum amount of data to be transported on behalf of the service flow when averaged over time. The specified rate SHALL only be honored when sufficient data is available for scheduling. When insufficient data exists, the requirement imposed by this parameter SHALL be satisfied by assuring the available data is transmitted as soon as possible.
Length	2+4
Value	Unsigned Integer specifying the rate in bytes.

TLV ID	8 for Maximum Traffic Burst
Description	Represents the Maximum Traffic Burst as defined in IEEE802.16e. This parameter defines the maximum burst size that SHALL be accommodated for the service. Since the physical speed of ingress/egress ports, the air interface, and the backhaul will in general be greater than the maximum sustained traffic rate parameter for a service, this parameter describes the maximum continuous burst the system should accommodate for the service assuming the service is not currently using any of its available resources.
Length	2+4
Value	Unsigned Integer specifying the burst size in bytes per second as defined by IEEE802.16e.

TLV ID	9 for Tolerated Jitter
Description	Represents the Tolerated Jitter as defined in IEEE802.16e.
Length	2+4
Value	Unsigned Integer representing the maximum delay variation (jitter) (in milliseconds).

TLV ID	10 for Maximum Latency
Description	Represents the Maximum Latency as defined in IEEE802.16e. Time period between the reception of a packet by the BS or MS on its network interface and the delivering the packet to the RF Interface of the peer device. If defined, this parameter represents a service commitment (or admission criteria) at the BS or MS and SHALL be guaranteed by the BS or MS. A BS or MS does not have to meet this service commitment for service flows that exceed their minimum reserved rate.
Length	2+4
Value	Unsigned Integer specifying a maximum latency in units of milliseconds.

TLV ID	11 for Reduced Resources Code
Description	This code indicates that the requesting entity will accept reduced resources if the requested resources are not available.
Length	2+1
Value	Unsigned Octet: value of 0 is not allowed, value of 1 allowed. Other values are reserved.

TLV ID	12 for Media Flow Type
Description	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
Length	2+1
Value	The first octet of the string represents an enumeration with the following values: • 0 = Reserved • 1 = Voice over IP • 2 = Robust Browser • 3 = Secure Browser/ VPN

	• 4 = Streaming video on demand • 5 = Streaming live TV • 6 = Music and Photo Download • 7 = Multi-player gaming • 8 = Location-based services • 9 = Text and Audio Books with Graphics • 10 = Video Conversation • 11 = Message • 12 = Control • 13 = Data • 14 – 255 = Reserved

TLV ID:	13 for Unsolicited Grant Interval
Description:	The value of this parameter specifies the nominal interval between successive data grant opportunities for this service flow. This parameter may be used for UGS and ERT-VR service flow when the inter-arrival time of IP packets on the data plane is known in advance (this is typically the case for flows generated by a specific codec).
Length:	2+2
Value:	Unsigned Short measuring time in milliseconds.

TLV ID	14 for SDU Size
Description	Represents the number of bytes in the fixed size SDU. This parameter may be used for a UGS service flow when the length of IP packets on the data plane is fixed and known in advance (this is typically the case for flows generated by a specific codec). If this attribute is absent then the SDU SHALL be variable.
Length	2+1
Value	8-bit unsigned integer. Default = 49.

TLV ID	15 for Unsolicited Polling Interval
Description	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
Length	2+2
Value	16-bit unsigned integer representing the polling interval (in milliseconds).

TLV ID	16 for Media Flow Description in SDP format
Description	This is a variable length string having SDP information. The <SDP string> is encoded as specified in IETF RFC 2327.
Length	2+String
Value	<SDP string> is encoded as specified in IETF RFC 2327.

TLV ID	17 for Transmission Policy
Description	The parameter indicates the transmission policy of a service flow.
Length	2+1
Value	Octet enumeration with the following values defined: • Bit #0 – Service flow SHALL NOT use broadcast bandwidth request opportunities. (Uplink only) • Bit #1 –Service flow SHALL NOT use multicast bandwidth request opportunities. (Uplink only). • Bit #2 – The service flow SHALL NOT piggyback requests with data. (Uplink only) • Bit #3 – The service flow SHALL NOT fragment data. • Bit #4 – The service flow SHALL NOT suppress payload headers (CS parameter). • Bit #5 – The service flow SHALL NOT pack multiple SDUs (or fragments) into single MAC PDUs. • Bit #6 – The service flow SHALL NOT include CRC in the MAC PDU. • Bit #7 – The service flow SHALL NOT compress payload headers using ROHC. All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits. Note: The bit#7 is reserved prior to WiMAX Forum® Network Architecture release 1.5

<table>
<tr><td><b>TLV ID</b></td><td>18 for DSCP</td></tr>
<tr><td><b>Description</b></td><td>Differentiated services code point as defined in RFC 2474 [30]. Used to mark the bearer IP packets of the flow on the R3 interface: ASN-GW marks the packets on the UL, CSN node marks the packets on the DL. Used to mark the IP packets of the flow. See RFC3246 [47], RFC2597 [35] and RFC4595 [77] for recommended values.</td></tr>
<tr><td><b>Length</b></td><td>2+1</td></tr>
<tr><td><b>Value</b></td><td>Unsigned Octet representing the DSCP field as defined in RFC2474 [30]
DSCP field as defined in RFC 2474 [30]
<pre>
     0   1   2   3   4   5   6   7
  +---+---+---+---+---+---+---+---+
  | DSCP | CU |
  +---+---+---+---+---+---+---+---+

    DSCP: differentiated services codepoint
    CU: currently unused
</pre></td></tr>
</table>

TLV ID	19 for Priority-Indication
Description	The parameter indicates the priority associated with a service flow.
Length	2+1
Value	Bit 0: Emergency indication Bits 1–7: *Reserved*

5.4.3.30 Uplink-Granted-QoS

```
    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  |  QoS Descriptor
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	30 for Uplink-Granted-QoS
Description	Uplink QoS granted to the MS.
Length	6+3+length of QoS-Descriptor
Continuation	C-bit = 0 or 1
Value	QoS Descriptor value

5.4.3.31 Control-Packets-In

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Continuation  |                 Value
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |
   +-+-+-+-+-+-+-+-+
```

WType-ID	31 for Control-Packets-In
Description	Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing packets count.

5.4.3.32 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |
   +-+-+-+-+-+-+-+-+
```

WType-ID	32 for Control-Octets-In
Description	Octet counts for incoming Mobile IPv4, DHCP, ICMP messages etc.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing octets.

5.4.3.33 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |
   +-+-+-+-+-+-+-+-+
```

WType-ID	33 for Control-Packets-Out
Description	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing packets count.

5.4.3.34 Control-Octets-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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |
   +-+-+-+-+-+-+-+-+
```

WType-ID	34 for Control-Octets-Out
Description	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing an octet count.

5.4.3.35 PPAC

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Continuation  |          TLV
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	35 for PPAC
Description	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.
Length	6 + 3 + TLVs
Continuation	C-bit = 0.
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	AvailableInClient (AiC)	2+4	1	0	0	0

TLV ID	1 for AvailableInClient (AiC)
Description	The optional AvailableInClient Subtype, generated by the PPC, indicates the metering capabilities of the NAS and SHALL be bit-map encoded. The possible values are as follows.
Length	2+4
Value	4 Octet String interpreted as a bit map with the following values: • Bit #0 - Volume metering supported • Bit #1 - Duration metering supported • Bit #2 - Resource metering supported • Bit #3 - Pools supported • Bit #4 - Rating groups supported • Bit #5 - Multi-Services supported • Bit #6 - Tariff Switch supported All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.4.3.36 Session Termination Capability

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |           4 Octet-String                                      |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	36 for Session Termination Capability
Description	This attribute is included in a RADIUS Access-Request packet to the RADIUS server and indicates whether or not the NAS supports Dynamic Authorization.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	4 octet Bit Map with the following values: • Bit #0 - Dynamic Authorization Extensions ([52]) is supported All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.4.3.37 PPAQ Attribute

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Continuation  |        TLV
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	37 for PPAQ
Description	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.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	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

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.

TLV ID	1 for Quota-Identifier
Description	It is generated by the PPS together with the allocation of new quota. The online quota update RADIUS Access-Request packet that is sent from the PPC to the PPS includes a previously received QuotaIdentifier AVP.
Length	2+Length of Quota-Identifier (Quota-Identifier not to exceed 4 octets)
Value	Octet String. The Quota-Identifier value (most significant bit first).

TLV ID	2 for Volume-Quota
Description	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).
Length	2+(8 or 12)
Value	• 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. • 4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field.

TLV ID:	3 for Volume-Threshold
Description:	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).
Length:	2+(8 or 12)
Value:	• 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. • 4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field.

TLV ID	4 for Duration-Quota
Description	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.
Length	2+4
Value	Unsigned Integer representing seconds.

TLV ID	5 for Duration-Threshold
Description	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.
Length	2+4
Value	Unsigned Integer representing seconds.

TLV ID	6 for Resource-Quota
Description	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).
Length	2+(8 or 12)
Value	• 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. • 4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field.

TLV ID	7 for Resource-Threshold
Description	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.
Length	2+(8 or 12)
Value	• 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. • 4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field.

TLV ID	8 for Update-Reason
Description	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.
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = Pre-initialization • 2 = Initial-Request • 3 = Threshold Reached • 4 = Quota Reached • 5 = TITSU Approaching • 6 = Remote Forced Disconnect • 7 = Client Service Termination • 8 = “Access Service” Terminated • 9 = Service not established • 10 = One-time Charging

TLV ID	9 for Prepaid-Server
Description	This optional AVP indicates the address (IPv4 or IPv6) of the serving PPS. If present, the Home RADIUS server uses this address to route the message to the serving PPS. The attribute may be sent by the Home RADIUS server. Multiple instances of this subtype MAY be present in a single PPAQ AVP. If present in the incoming RADIUS Access-Accept 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.
Length	2 + (4 (IPv4) or 16 (IPv6))
Value	The value of this AVP is encoded as an IPv4 address or an IPv6 address.

TLV ID	10 for Service-ID
Description	This value is a string that uniquely describes the service instance to which prepaid metering should be applied. The format of the Service-Id is: "tag"."service identifier". The "tag" indicates the additional feature of the service, e.g. ALR is enabled or not. A service identifier 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. There are two Service-IDs for a local routing enabled service: one for the normal traffic and one for the local-routed traffic. The latter is identified by an ALR tag. If a Service-ID AVP is present in the PPAQ, the entire PPAQ refers to that service. If a PPAQ does not contain a Service-Id or Rating-Group-ID, then the PPAQ refers to the Access Service (ISF).

	For IP Session based accounting only one Service-ID (or two Service-IDs in case of local routing enabled) encoded as below SHALL be included.
Length	2+ Length of Service-ID
Value	The value field of this AVP is encoded as a UTF8 string as follows: The tag for ALR is "ALR". Other string values are reserved for future use. To encode an IP-Tuple for flow based accounting the syntax used in the IPFilterRule of RFC3588 is used as follows: "iptuple=" dir proto "from" src "to" dst 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: "pdfid="pdfid1 (encoding if there is one PDFID) OR "pdfid= "pdfid1,pdfid2,… (encoding if there are two or more PDFIDs) where: pdfid is the ascii hex representation of the PDFID as in (0xfada) To encode one or more SDFIDs: "sdfid="sdfid1 (encoding if there is one SDFID) OR "sdfid=" sdfid1,sdfid2,… (encoding if there are two or more SDFIDs) where: sdfid is the ascii hex representation of the SDFID as in (0xfada) For IP session based accounting : IP Address is encoded as ASCII hex using IPFilterRule format of 3588. "assigned" if IP address is unknown or ASCII version of IP address i.e. "1.2.3.4".

1

TLV ID	11 for Rating-Group-ID
Description	This AVP indicates that this PPAQ is associated with resources allocated to a Rating Group with the corresponding ID. This AVP is encoded as a string. A PPAQ SHALL NOT contain more than one Rating-Group-ID.
Length	2+4
Value	Unsigned Integer representing the value of the Rating Group ID.

2

TLV ID	12 for Termination-Action
Description	This AVP describes action to take when the PPS does not grant additional quota.
Length	2+1
Value	Octet Enumeration with the following values: • 0 = Reserved • 1 = Terminate • 2 = Request more quota • 3 = Redirect/Filter

3

TLV ID	13 for Pool-ID
Description	This AVP identifies the resource pool that the quota included in this PPAQ is associated with.
Length	2+4
Value	Unsigned Integer representing a Pool-ID.

TLV ID	14 for Pool-Multiplier
Description	The pool-multiplier determines the weight that resources are inserted into the pool that is identified by the accompanying Pool-ID AVP, and the rate at which resources are taken out of the pool by the relevant Service or Rating-Group. It consists of a Value-Digits field and optionally an Exponent field (as indicated by the length field).
Length	2+(8 or 12)
Value	• 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. • 4 octets = Exponent field is a Integer32 value which contains the exponent value to be applied for the Value-Digits field

TLV ID	15 for Requested-Action
Description	This AVP can only be present in messages sent from the PPC to the PPS. It indicates that the user or the PPC desires the PPS to perform the indicated action and to return the result. The PPAQ in which a Requested-Action AVP occurs SHALL NOT contain a Quota-Identifier, and SHALL 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.
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = Balance Check • 2 = Price Enquiry

TLV ID:	16 for Check-Balance-Result
Description:	This AVP can only be present in messages sent from the PPS to the PPC. It indicates the balance check decision of the PPS about a previously received Balance Check Request (as indicated in a Requested-Action AVP).
Length:	2+1
Value:	Octet enumeration with the following values: • 0 = Success • Any other value = Failure

TLV ID	17 Cost-Information
Description	This AVP is used in order to return the cost information of a service as specified by the Service-ID, which the PPC can transfer transparently to the end user. This AVP is sent from the PPS to the PPC as a response to a "Price Enquiry", as indicated by the Requested-Action AVP. If Cost-Information is not available for the specified Service-ID, then the Cost-Information AVP SHALL NOT appear in the response.
Length	2 + 16 + length of cost-unit
Value	The value is encoded using fixed encoding and consists of the following fields: • 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. For example, for the monetary amount $ 0.05 the value of Value-Digits AVP MUST be set to 5, and the scaling MUST be indicated with the Exponent AVP set to -2. • 4 octets = Exponent field is an Integer32 value which contains the exponent value to be applied for the Value-Digits field. • 4 octets = Currency-Code field is an Unsigned32 value which contains a currency code that specifies in which currency the values of AVPs containing monetary units were given. It is specified by using the numeric values defined in the ISO 4217 standard [ISO4217]. • 0 or more octets = Cost-Unit is a UTF8String encoded human readable string that can be displayed to the end user. It specifies the applicable unit to the Cost-Information when the service cost is a cost per unit (e.g., cost of the service is $1 per minute). The Cost-Unit can be minutes, hours, days, kilobytes, megabytes, etc.

5.4.3.38 Prepaid Tariff Switching Attribute (PTS)

```
   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  |        TLVs
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	38 for Prepaid Tariff Switching (PTS)
Description	PTS attribute which allows for changeovers from one rate to another during service provision. Support for tariff switching is optional for both the PPC and the PPS. PPCs use the flag "Tariff Switching supported" of the PPAC attribute in order to indicate support for tariff switching.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	Quota Identifier	2+Length	1	1	0	0
2	VolumeUsedAfterTariffSwitch	2+(8 or 12)	1	0	0	0
3	TarrifSwitchInterval	2+4	0	0-1	0	0
4	TimeIntervalAfterTarriffSwitchUpdate	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.

TLV ID	1 for Quota Identifier
Description	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.
Length	2+4
Value	Octet String. The Quota Identifier value (most significant bit first)

TLV ID	2 for VolumeUsedAfterTariffSwitch
Description	Indicates the volume (in octets) used during a session after the last tariff switch for the service specified via the QID subfield and the accompanying PPAQ attribute.
Length	2+(8 or 12)
Value	Unsigned Integer representing a number of kilo-octets (1024 octets).

TLV ID	3 for TarrifSwitchInterval
Description	Indicates the interval (in seconds) between the value of Event-Timestamp RADIUS attribute (see [41]) of the corresponding RADIUS Access-Request packet and the next tariff switch condition.
Length	2+4
Value	Unsigned Integer indicating a number of seconds.

TLV ID	4 for TimeIntervalAfterTarriffSwitchUpdate
Description	Contains the number of seconds of the tariff period that begins immediately after the period that ends as indicated by the TarriffSwitchInterval sub-TLV. If the TITSU attribute is not present, the PPC assumes that the tariff period which ends as indicated by the TSI attribute lasts until further notice. If TITSU is specified, the PPC SHALL send a quota update before the point in time specified by the TITSU attribute.
Length	2+Length of Quota Identifier
Value	Unsigned Integer measuring a number of seconds.

5.4.3.39 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |               |
   +-+-+-+-+-+-+-+-+
```

WType-ID	39 for Active-Time
Description	The amount of time the session was not in Idle state.
Length	6 + 3 +4
Continuation	C-bit = 0
Value	Unsigned Integer. The time in seconds.

5.4.3.40 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	40 for hDHCP-RK
Description	The hDHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted hDHCP-RK.
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2 octet SALT (see [40]) and String containing the encrypted hDHCP-RK formulated as per [40].

5.4.3.41 hDHCP-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 DHCP-RK
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                   |
   +-+-+-+-+-+-+-+-+
```

WType-ID	41 for hDHCP-RK-Key-ID
Description	An integer number uniquely identifying the hDHCP-RK within the scope of a single DHCP server.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

5.4.3.42 hDHCP-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 DHCP-RK
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	42 for hDHCP-RK-Lifetime
Description	Lifetime of the hDHCP-RK and derived keys.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

5.4.3.43 DHCPMSG-Server-IP

```
 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  |     DHCP server addr.
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	43 for DHCPMSG-Server-IP
Description	The IPv4 address of the DHCP server contained in the DHCPDISCOVER message.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing an IPv4 address of DHCP server (most significant bit first) to which the DHCPDISCOVER/DHCPREQUEST message was sent.

5.4.3.44 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     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	44 for Idle-Mode-Transition
Description	A flag indicating whether the mobile node is in idle or not.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Unsigned Octet. When set to (1) the MS is in idle mode. When set to (0) the MS is not in Idle mode.

5.4.3.45 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                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	45 for NAP-ID
Description	Uniquely identifies the Network Access Provider.
Length	6 + 3 + 3
Continuation	C-bit = 0.
Value	Octet-String (3 Octets) representing an operator identifier.

5.4.3.46 BS-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                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                BS - ID                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	46 for BS-ID
Description	Uniquely identifies a NAP and a Base Station within that NAP.
Length	6 + 3 + 6
Continuation	C-bit = 0
Value	Octet-String (6 Octets). Representing NAP operator identifier (first 3 Octets) and the Base Station ID (next 3 Octets).

5.4.3.47 Location

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |          Vendor-ID            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |                 Location
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	47 for Location
Description	Location of the ASN.
Length	6 + 3 + Length of Location (>0)
Continuation	C-bit = 0 or 1
Value	Octet-String representing location. Format is 0.

5.4.3.48 Acct- Input -Packets-Gigaword

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Continuation  |                 Location
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	48 for Acct- Input -Packets-Gigaword
Description	Number of packets incremented each time Acct- Input -Packets(47) overflows.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing 2^{32} packets counts.

5.4.3.49 Acct- Output -Packets Gigaword

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Continuation  |                 Location
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	49 for Acct- Output -Packets-Gigaword
Description	Number of packets incremented each time Acct- Output -Packets(48) overflows.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer representing 2^{32} packets counts.

5.4.3.50 Uplink Flow Description

```
    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  |         Uplink   Flow Description
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	50 for Uplink Flow Description
Description	Describes an Uplink flow classifier.
Length	6+3 + Length of Uplink Flow Description
Continuation	C-bit = 0
Value	String containing an IP-Filter Rule as pre RFC3588. Action is set to ”permit”.

5.4.3.51 BU-CoA-Ipv6

```
 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  |                 BU-CoA-IPv6
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                  |
+-+-+-+-+-+-+-+-+-+
```

WType-ID	51 for BU-CoA-IPv6
Description	The CoA from the BU message.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet-String representing an IPv6 address most significant octet first.

5.4.3.52 DNS

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |          Vendor-ID            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |                 DNS
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                  |
+-+-+-+-+-+-+-+-+-+
```

WType-ID	52 for DNS
Description	The IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.
Length	6 + 3 + (4 for IPv4 or 16 for IPv6)
Continuation	C-bit = 0
Value	Octet-String representing an IPv4 or IPv6 address most significant octet first.

5.4.3.53 Hotline-Profile-ID

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Continuation  |                 String
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	53 for Hotline-Profile-ID
Description	A unique identifier (relative to the HCSN) of a Hot-Line profile to be applied to this session.
Length	6 + 3 + length of octet-string.
Continuation	C-bit = 0
Value	String representing a Hot-Line profile formatted as follows: realm + "/" + profile-id-string Where: • Realm is the Fully Qualified Domain Name of the operator that is asserting the Hot-Line profile; and • Profile-id-string is operator specific label for the Hot-Line profile to be applied at the by the Hot-Lining device.

5.4.3.54 HTTP-Redirection-Rule

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Continuation  |                 string
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	54 for HTTP-Redirection-Rule
Description	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

<table>
<tr><td></td><td>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.
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 following HTTP redirection rule forces any HTTP requests from the MS to http://www.wimaxforum.org/home:
redirect http://www.wimaxforum.org in ip from assigned to any 80
The first redirect results in the MS browser sending the original HTTP request to 66.179.20.189, which is the IP for http://www.wimaxforum.org. But this redirected HTTP request will generate IP packet that triggers another redirect to the same URL, http://www.wimaxforum.org 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”.
In order to avoid the HTTP redirection loops, the following requirements need to be met during the provisioning of HTTP redirection rules:
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 http://www.wimaxforum.org in ip from assigned to any 80
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 http://www.wimaxforum.org in ip from assigned to 66.179.20.0/8 80</td></tr>
<tr><td><b>Length</b></td><td>6 + 3 + length of rule.</td></tr>
<tr><td><b>Continuation</b></td><td>C-bit = 0</td></tr>
<tr><td><b>Value</b></td><td>An string formatted as per IPFilterRule specified by [55] with the following exception:
The action portion of the rule SHALL follow the following:
<table>
<tr><td>Action Keyword</td><td>Description</td></tr>
<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>
</table></td></tr>
</table>

5.4.3.55 IP-Redirection-Rule

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |          Vendor-ID            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |                 string
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

<table>
<tr><td><b>WType-ID</b></td><td>55 for IP Redirection Rule.</td></tr>
<tr><td><b>Description</b></td><td>The IPv4/IPv6 address of the DNS server to be conveyed to the MS via DHCP.</td></tr>
<tr><td><b>Length</b></td><td>6 + 3 + length of rule</td></tr>
<tr><td><b>Continuation</b></td><td>C-bit = 0</td></tr>
<tr><td><b>Value</b></td><td>An string formatted as per IPFilterRule specified by [55] with the following exception:
The action portion of the rule SHALL follow the following:
<table>
<tr><td>Action Keyword</td><td>Description</td></tr>
<tr><td>"redirect" IP[port]</td><td>If the rule matches then redirect packets that match the rule to the specified IP address and optional port.</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>
</table>
</td></tr>
</table>

5.4.3.56 Hotline-Session-Timer

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |          Vendor-ID            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |            unsigned integer
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|               |
+-+-+-+-+-+-+-+-+
```

WType-ID	56 for Hotline-Session-Timer
Description	The length of time in seconds the session can remain hotlined. If not specified the length of time the session is hotlined is determined by the Session-Time and Termination-Action attributes. Session-Time with Termination-Action set to Default(0) SHALL override this timer. If Session-Time with Termination-Action is set to RADIUS-Request(1), the NAS SHALL reauthenticate without resetting the value of Hotline-Session-Timer. Upon successful reauthentication, if the NAS receives a new Hotline-Session-Timer value, the NAS SHALL terminate the session based on the value specified by the received attribute.
Length	6 + 3 + 4
Continuation	C-bit = 0

Value	Unsigned Integer representing a time in seconds. A value of zero means infinity.

5.4.3.57 NSP-ID

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |   Length      |          Vendor-ID            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | Continuation  |                 Operator ID                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	57 for NSP-ID
Description	Uniquely identifies the Network Service Provider.
Length	6 + 3 + 3
Continuation	C-bit = 0.
Value	Octet-String (3 Octets) representing an operator identifier.

5.4.3.58 Void

5.4.3.59 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       |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	59 for Count-Type
Description	Used to indicate if the record represents compressed or uncompressed counts.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Unsigned Octet. When set to (0) indicates uncompressed counts. When set to (1) indicates compressed counts.

5.4.3.60 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                   |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |               |
   +-+-+-+-+-+-+-+-+
```

WType-ID	60 for WiMAX-DM-Action-Code
Description	This attribute indicates the deregistration action to take when the NAS receives a Disconnect Message.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned Integer. Enumerator. The values are: • 0x0000 = Deregister MS/AMS. MS/AMS SHALL immediately terminate service with the BS/ABS and should attempt network entry at another BS/ABS. • 0x0001 = Suspend all MS/AMS traffic including control traffic. MS/AMS SHALL listen to the current BS/ABS but SHALL NOT transmit until an RES-CMD/AAI-RES-CMD message or DREG-CMD/AAI-DREG-RSP with Action Code 02 or 03 is received. • 0x0002 = Suspend user traffic (transport connections). MS/AMS SHALL listen to the current BS/ABS but only transmit on the Basic and Primary Management Connections. • 0x0003 = Resume traffic. MS/AMS SHALL return to normal operation and may transmit on any of its active connections. • 0x0004 = Reserved. • 0x0005 = MS/AMS SHALL be put into idle mode. • 0x0006 = MS/AMS successfully completed MIP6 handover. • 0xFFFF = MS/AMS SHALL be sent the RES-CMD/AAI-RES-CMD by the BS/ABS. The MS/AMS will reload all configuration information and do initial network entry. • 0x0007 - 0xFFFE = Reserved.

5.4.3.61 FA-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  |                 TLV
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	61 for FA-RK-SPI
Description	The SPI used for the FA-RK.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

5.4.3.62 Downlink Flow Description

```
    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  |      Downlink  Flow Description
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	62 for Downlink Flow Description
Description	Describes a flow classifier for the downlink.
Length	6+3 + Length Downlink Flow Description
Continuation	C-bit = 0
Value	String containing an IP-Filter Rule as pre RFC3588. Action is set to ”permit”.

5.4.3.63 Downlink-Granted-QoS

```
    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  |    QoS Descriptor
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	63 for Downlink-Granted-QoS
Description	Downlink QoS granted to the MS.
Length	6+3 + Length of QoS-Descriptor
Continuation	C-bit = 0 or 1
Value	QoS Descriptor value

5.4.3.64 vHA-IP-MIP4

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |  Length       |            Vendor-Id          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Continuation |   HA-IP
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	64 for vHA-IP-MIP4
Description	The IPv4 address of the vHA for MIP4.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing an IPv4 address (most significant bit first).

5.4.3.65 vHA-IP-MIP6

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |  Length       |            Vendor-Id          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Continuation |   HA-IP
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	65 for vHA-IP-MIP6
Description	The IPv6 address of the vHA for MIP6.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet string containing an IPv6 address (most significant bit first).

5.4.3.66 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	66 for MN-vHA-MIP4-KEY
Description	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.
Length	6 + 3 +2(SALT)+ Length of the encrypted MN-vHA-MIP4-KEY
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2 octet SALT (see [40]) and String containing the encrypted MN-vHA-MIP4-KEY formulated as per [40].

5.4.3.67 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	67 for vHA-RK-KEY
Description	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.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted vHA-RK-KEY.
Continuation	When following the procedures defined in [40] 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.
Value	The value consists of 2-octet SALT (see [40]) and String containing the encrypted vHA-RK formulated as per [40].

5.4.3.68 vHA-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  |     TLV
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	68 for vHA-RK-SPI
Description	The SPI used for the vHA-RK.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

5.4.3.69 vHA-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  |     TLV
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	69 for vHA-RK-Lifetime
Description	The Lifetime of the vHA-RK and derived keys.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first representing the time before the key expires in seconds.

5.4.3.70 MN-vHA-MIP4-SPI

```
  0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Continuation  |              SPI                              |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |               |
 +-+-+-+-+-+-+-+-+
```

WType-ID	71 MN-vHA-MIP4-SPI
Description	The SPI associated with the MN-vHA-MIP4-KEY.
Length	6+3+4
Continuation	C-bit = 0
Value	Unsigned 32-bit Integer. In an Access-Accept sent from the home AAA to the ASN the value is set to SPI-PMIP4.

5.4.3.71 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	73 for vDHCPv4-Server
Description	The IPv4 address of the visited DHCP-Server to use for IPv4 address allocation by the vASN.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing an IPv4 address (most significant bit first).

5.4.3.72 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	74 for vDHCPv6-Server
Description	The IPv6 address of the visited DHCP-Server to use for IPv6 allocation by the vASN.
Length	6 + 3 +16
Continuation	C-bit = 0
Value	Octet string containing an IPv6 address (most significant bit first).

5.4.3.73 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	75 for vDHCP-RK
Description	The vDHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
Length	6 + 3 + 2(SALT) + length of the String containing the encrypted vDHCP-RK.
Continuation	When following the procedures defined in [40]. 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.
Value	The value consists of 2 octets for the SALT (see [40]) And a String containing the encrypted vDHCP-RK formulated as per [40].

5.4.3.74 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
                |
+-+-+-+-+-+-+-+-+
```

WType-ID	76 for vDHCP-RK-Key-ID
Description	An integer number uniquely identifying the vDHCP-RK within the scope of a single DHCP server.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

5.4.3.75 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	77 for vDHCP-RK-Lifetime
Description	Lifetime of the vDHCP-RK and derived keys.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

5.4.3.76 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
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	78 for PMIP-Authenticated-Network-Identity
Description	Authenticated identity of the MS/AMS.
Length	6+3 + length of NAI
Continuation	C-bit = 0
Value	Octet string containing Identity of the MS/AMS in NAI format.

5.4.3.77 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
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	79 for Visited-Framed-IP-Address
Description	The IPv4 Address assigned by the Visited CSN to be used for the MS/AMS.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing an IPv4 address (most significant bit first).

5.4.3.78 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	80 for Visited-Framed-IPv6-Prefix
Description	The IPv6 prefix assigned by the Visited CSN to be used for the MS/AMS.
Length	(6 + 3) +1+(0-16)
Continuation	C-bit = 0
Value	Octet string contains one byte of "Prefix-Length" and up to 16 bytes of Visited-Framed-IPv6-Prefix.

5.4.3.79 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	81 for Visited-Framed-Interface-Id
Description	The IPv6 interface Id assigned by the Visited CSN to be used for the MS/AMS.
Length	6 + 3 + 8
Continuation	C-bit = 0
Value	Octet string containing an IPv6 address (most significant bit first)

5.4.3.80 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |               |
   +-+-+-+-+-+-+-+-+
```

WType-ID	82 for MIP-Authorization-Status
Description	This attribute when set to ‘true’ means AAA is authorizing the MS to use MIP6. ‘False’ means the MS is not authorized.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	The value is an unsigned 32-bit integer. If the value is set to 1 (TRUE) then the AAA has authorized the MS/AMS to use MIP6. If the value is set to 0 (FALSE) then the AAA has not authorized the MS/AMS to use MIP6.

5.4.3.81 Flow-Description-V2

```
   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  |         Flow Description
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	83 for Flow-Description-V2
Description	Describes a classifier of a flow.
Length	6+3 + Length of classifier TLV
Continuation	C-bit = 0
Value	A classifier encoded using TLVs as described in section 5.4.2.84.

5.4.3.82 Packet-Flow-Descriptor-V2

```
   0                   1                   2                   3
   0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |RADIUS TYPE 26 |  Length       |             Vendor-Id         |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
  |  Continuation |               TLV
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	84 for Packet-Flow-Descriptor-V2
Description	This attribute describes a packet flow. A packet flow may describe a uni-directional flow and bidirectional flow. The packet flow descriptor may be pre-provisioned. A packet flow descriptor references one or two QoS specifications. 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.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

1

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR	CoA
1	PacketDataFlowID	2+2	0	1	0	0	1
2	ServiceDataFlowID	2+2	0	0-1	0	0	0-1
3	ServiceProfileID	2+4	0	0-1[a]	0	0	0-1[a]
4	Direction	2+1	0	0-1[b][i]	0	0	0-1[b]
5	ActivationTrigger	2+1	0	0-1[b][i]	0	0	0-1[b]
6	TransportType	2+1	0	0-1[b]	0	0	0-1[b]
7	UplinkQosID	2+1	0	0-1 [c][i]	0	0	0-1 [c]
8	DownlinkQoSID	2+1	0	0-1 [d]	0	0	0-1 [d]
9	Classifier[42]	2+Length	0	0-n	0	0	0-n
10	Paging-Preference	2+1	0	0-1[e][i]	0	0	0-1[e]
11	VLANTagProcessingRuleID	2+2	0	0-1[f]	0	0	0-1[f]
12	SF-Operation-Policy	2+1	0	0-1[g]	0	0	0-1[g]
13	Local-Routing-Policy	2+1	0	0-1[h]	0	0	0-1[h]
14	Start Time	2+Length	0	0-1[j]	0	0	
15	End Time	2+Length	0	0-1[j]	0	0	
16	MCBCS Service Continuity Indicator	2+1	0	0-1[j]	0	0	

[42] Classifier defined within Packet Flow Descriptor maps to “Classification Rule” defined over R4/R6 interfaces

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/AMS.

[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/AMS.

[d] This attribute SHALL be present if SerivviceProfileID 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/AMS.

([e]) This attribute is applicable to the downlink service flow only.

[f] This attribute may only be present for Ethernet service flows.

[g] This attribute may only be present when the PDF/PCRF or the AAA and the serving ASN support the per SF Operation Policy that is used to indicate the encryption operation policy on per SF basis. If the ASN has indicated the support of the SF airlink encryption on/off capability, the “absence” of this TLV implies that the airlink encryption on/off policy for the given service flow is a local implementation policy of the ASN.

[h] This attribute may only be present when the PDF/PCRF or the AAA and the ASN support the Local Routing Policy.

[i] This attribute is not applicable for MCBCS service.

[j] This attribute is applicable for MCBCS service.

TLV ID	1 for PacketDataFlow-ID
Description	This attributes identifies a packet data flow instance. The identifier is assigned by the home network and is unique per mobile session or per MCBCS flow for the entire session. PacketDataFlow-IDs 1 to 20 are assigned for the packet data flow of the Initial Service Flow (ISF). The PacketDataFlow-ID, along with the MCBCS transmission zone ID is used to uniquely identify an MCBCS service.
Length	2+2
Value	Unsigned Short representing the flow identifier (most significant bit first). A value of zero(0) is invalid.

TLV ID	2 for ServiceDataFlow-ID
Description	This attribute is used to group of one or more packet data flows belonging to the same service instances (e.g., a combined voip/video call). The number is assigned by the home network and is unique per mobile session or per MCBCS flow 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.

Length	2+2
Value	Unsigned Short representing the Service flow identifier (most significant bit first). This value is assigned by the home network and is unique per mobile session for the life of the session. A value of zero(0) is invalid.

TLV ID	3 ServiceProfileID
Description	This attribute identifies a pre-configure flow descriptor at the NAS.
Length	2+4
Value	Unsigned Integer representing the identity of a Flow Spec that is pre-provisioned (most significant bit first). A value of zero(0) is invalid.

TLV ID	4 for Direction
Description	The direction of the Packet Data Flow.
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = Uplink • 2 = Downlink • 3 = Bi-directional • 4 – FF = Reserved

TLV ID	5 for ActivationTrigger
Description	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.
Length	2+1
Value	Octet bit-map with the following values: • Bit #0 - Provisioned (SHALL be set in case of ISF) • Bit #1 - Admit (SHALL be set in case of ISF) • Bit #2 - Activate (SHALL be set in case of ISF) • Bit #3 - Dynamic Reservation (not valid for ISF) All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits. If "Dynamic Reservation" is set to false, the QoS-Descriptor is used to specify a QoS profile for ISFs or pre-provisioned SFs. 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.

TLV ID	6 for TransportType
Description	Defines the transport type which might be IP (v4 or v6) as well as Ethernet. This parameter need to be mapped into "CS specification" as defined in IEEE802.16e/m [REF1].
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = IPv4-CS • 2 = IPv6-CS • 3 = Ethernet • 4 – 255 = Reserved

TLV ID	7 for UplinkQoSID
Description	The identifier of the QoS descriptor for the uplink direction or for bi-direction if the flow is bi-directional with symmetrical QoS. If the QoSID is not resolvable by the NAS, the NAS SHALL reject the network entry of the MS/AMS.
Length	2+1
Value	Unsigned Octet containing the ID of the QoS descriptor.

TLV ID	8 for DownlinkQoSID
Description	The identifier of the QoS descriptor for the downlink direction. If the QoSID is not resolvable by the NAS, the NAS SHALL reject the network entry of the MS.
Length	2+1
Value	Unsigned Octet containing the ID of the QoS descriptor.

TLV ID	9 for Classifier
Description	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/AMS.
Length	2+Variable
Value	Contains a set of nested TLVs describing IP classifiers.

TLV ID	10 for Paging-Preference
Description	This parameter is a single bit indicator of an MS/AMS's preference for the reception of paging advisory messages during idle mode. When set, it indicates that the BS/ABS may

	present paging advisory messages or other indicative messages to the MS/AMS when data SDUs bound for the MS/AMS are present while the MS/AMS is in idle mode.
Length	2+1
Value	Refer to 802.16e section 11.13.30.

TLV ID	11 for VLANTagProcessingRuleID
Description	The ID of the rules for assigning priority bits and VLAN-IDs in Ethernet frames
Length	2+2
Value	Unsigned-Short containing the VLANTagProcessingRuleID of the rules for processing the VLAN tags in Ethernet frames

TLV ID	12 for SF-Operation-Policy
Description	The value of this optional parameter is to specify the per SF operation policy.
Length	2+2
Value	One octet bit mask with the following values: Bit-0 = "0" - airlink encryption to be disabled during the SF creation. Bit-0 = "1" - airlink encryption to be enabled during the SF creation. If the ASN has indicated the support of the SF airlink encryption on/off capability, the "absence" of this TLV implies that the airlink encryption on/off policy for the given service flow is a local implementation policy of the ASN. Bit-1 to 7 = Reserved. The sender shall clear the reserved bits and the receiver shall ignore the reserved bits.

TLV ID	13 for Local-Routing-Policy
Description	Used to specify the Local Routing policy.
Length	2+1
Value	Enumerator. The values are: - 0x00=no ALR - 0x01=Pre-Authorized ALR - 0x02=Dynamic-Authorized ALR - - All other values are Reserved.

TLV ID	14 for Start Timer
Description	The time of packet data flow start; (UTC time format).
Length	2+Length of time
Value	Unsigned Short representing the start time of the MCBCS data flow.

TLV ID	15 for End Timer

Description	The time of packet data flow End; (UTC Time format).
Length	2+Length of time
Value	Unsigned Short representing the stop time of the MCBCS data flow.

TLV ID	16 for MCBCS Service Continuity Indicator
Description	Defines whether service continuity is supported among MBS Zones which belong to the same MCBCS Transmission Zone.
Length	2+1
Value	Octet enumeration with the following values: - 0 = Not supported - 1 = Supported - others = Reserved

5.4.3.83 Classifier

```
     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
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | TLV-ID 9 or 10|  LENGTH       |    TLV-ID 1   |   LENGTH  = 3 |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | classifier id | TLV-ID 2      |   LENGTH  = 3 |  protocol     |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | TLV-ID 3      |   LENGTH  = 3 |  direction    | . . . . .
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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
7	IP TOS/DSCP Range and Mask	2+3	0-1
8	Action	2+1	1
9	ETH-Option	2+Variable	0-1[b]

Notes:

[a] Classifier ID is unique within the parent container.

[b] May only present in case of Ethernet based transport.

TLV ID	1 for Classifier ID
Description	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.
Length	2+1
Value	0 to 255.

TLV ID	2 for Priority
Description	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.
Length	2+1
Value	Unsigned 8-bit integer. The higher the value the higher the priority.

TLV ID	3 for Protocol
Description	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.
Length	2+1
Value	Unsigned 8-bit integer. The encoding of the value field is that defined by the IANA document “Protocol Numbers.”

TLV ID	4 for Direction
Description	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.
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = IN (from the terminal) • 2 = OUT (to the terminal) • 3 = Bi-directional 4 – FF = Reserved.

TLV ID	5 for Source-Specification
Description	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.
Length	2+Variable
Value	Contains a nested TLV describing a source specification.

TLV ID	6 for Destination-Specification
Description	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.
Length	2+Variable
Value	Contains a nested TLV describing a destination specification.

TLV ID	7 for IP TOS/DSCP Range and Mask
Description	The values of the field specify the matching parameters for the IP type of service/DSCP [IETF RFC 2474] byte range and mask. An IP packet with IP type of service (ToS) byte value “ip-tos” matches this parameter if tos-low less than or equal (ip-tos AND tos-mask) less than or equal tos-high. If this field is omitted, then comparison of the IP packet ToS byte for this entry is irrelevant.
Length	2+3
Value	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.

TLV ID	8 for Action
Description	The value of this field specifies the action to either allow packets that match the rule or drop packets that match the rule.
Length	2+1
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = Permit – Allow Packets that match the rule. • 2 = Deny – Drop packets that match the rule. 3 – FF = Reserved

TLV ID	9 for ETH Option
Description	A grouped TLV with Ethernet specific attributes.

Length	2+Variable
Value	Contains a set of nested TLVs describing the Ethernet specific classifiers.

5.4.3.84 Source/Destination Specification

```
    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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | TLV-ID 4      |  LENGTH       |    TLV-ID 1   |   LENGTH  = 6 |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |                      ipv4 address                             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | TLV-ID 5      |   LENGTH  = 4 |  start port number            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   | end port number               |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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/AMS.

[e] Only valid for ETH-CS.

TLV ID	1 for IPAddress
Description	Specifies an IPv4 or IPv6 address to match. IPv4 and IPv6 addresses must not be both specified.
Length	2+4 octets for IPv4 Address or 2+ 16octets for IPv6 address
Value	A value representing an IPv4 address or an IPv6 address.

TLV ID	2 for IPAddressRange
Description	Specifies and IPv4 or an IPv6 address range to match. The range is inclusive. Both values MUST be IPv4 or IPv6.
Length	2+8 for IPv4 Address range or 2+32 for IPv6 Address range
Value	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.

TLV ID	3 for IPAddressMask
Description	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.
Length	2+5 For IPv4 block of addresses or 2+17 for an IPv6 block of addresses.
Value	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.

TLV ID	4 for Port
Description	Represent an IP port.
Length	2+2 Octets
Value	16-bit unsigned integer representing port numbers.

TLV ID	5 for Port Range
Description	Represents an inclusive port range consisting of a star port and an end port.
Length	2+4 Octets
Value	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.

TLV ID	6 for Inverted
Description	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 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 IPAddressRange1 AND NOT IPAddressMask1.
Length	2+1
Value	One octet representing boolean. 0 for false, 1 for true.

TLV ID	7 for Assigned
Description	If present indicates to use the assigned address(es) for the mobile in the source specification or destination specification or both.
Length	2+1 octets
Value	Unsigned 8-bit enumeration with values defined as follows: • 1 indicating the Source Assigned • 2 indicating the Destination Assigned • 3 indicates Source and Destination Assigned Other values are reserved.

TLV ID	8 for MAC address
Description	The value of this field specifies the MAC address
Length	2+6
Value	A value representing a MAC address

TLV ID	9 for MAC mask
Description	The value of this field specifies the MAC mask
Length	2+6
Value	A value representing a MAC mask

5.4.3.85 ETH Option

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | TLV-ID 9      |  LENGTH       |    TLV-ID 1   |     LENGTH    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | ETH Proto Type                |    TLV-ID 2   |     LENGTH    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | ETH VLAN ID                   |    TLV-ID 3   |     LENGTH    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | ETH Priority Range            |                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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

TLV ID	1 for ETH Proto Type
Description	Specifies Ethertype and DSAP.
Length	2+Variable
Value	Contains a nested TLV describing ETH Protocol Type

TLV ID	2 for ETH VLAN ID
Description	If present, this field specifies the matching values for the VLAN-ID bits. If omitted, the VLAN-ID bits are irrelevant for this entry.
Length	2+Variable
Value	Contains a nested TLV describing the VLAN-ID.

TLV ID	3 for ETH Priority Range
Description	If present, the priority SHALL match to the packet as specified in IEEE802.1D
Length	2+Variable
Value	Contains a set of nested TLVs describing the Ethernet Priority.

5.4.3.86 ETH Proto 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| TLV-ID 1      |  LENGTH       |    TLV-ID 1   |    LENGTH=4   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|           Ethertype           | TLV-ID 2      |    LENGTH=3   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    DSAP       |
+-+-+-+-+-+-+-+-+
```

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.

TLV ID	1 for ETH Ethertype
Description	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.
Length	2+2 octets
Value	16 bit representation of the Ethertype which SHALL match with the target.

TLV ID	2 for DSAP
Description	Specifies the Destination Service (DSAP) when SDUs using IEEE802.2 encapsulation format (DSAP other than 0xAA) is used.
Length	2+1 octets
Value	The octet represents the DSAP which SHALL match with the target.

5.4.3.87 ETH VLAN 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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | TLV-ID 2      |  LENGTH       |    TLV-ID 1   |   LENGTH=4    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |             S-VID             |    TLV-ID 2   |   LENGTH=4    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |             C-VID             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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.

TLV ID	1 for S-VID
Description	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]
Length	2+4 octets
Value	Only the lower 12 bits of the 2 byte value are significant; the upper four bits SHALL be ignored.

TLV ID	2 for C-VID
Description	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]
Length	2+4 octets
Value	Only the lower 12 bits of the 2 byte value are significant; the upper four bits SHALL be ignored.

5.4.3.88 ETH Priority Range

```
  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
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | TLV-ID 3      |  LENGTH       |     TLV-ID 1    |   LENGTH=3    |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 | Low Priority  |  TLV-ID 2     |    LENGTH=3     | High Priority |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

TLV ID	TLV Name	Length Octets	Occurrence
1	ETH Low Priority	2+1	0-1
2	ETH High Priority	2+1	0-1

TLV ID	1 for ETH Low Priority
Description	Lowest priority as specified in IEEE802.1D where a packet SHALL match to.
Length	2+1 octets
Value	Priority as specified in IEEE802.1D with a valid range from 0 to 7.

TLV ID	2 for ETH High Priority
Description	Highest priority as specified in IEEE802.1D where a packet SHALL match to.
Length	2+1 octets
Value	Priority as specified in IEEE802.1D with a valid range from 0 to 7.

5.4.3.89 VLANTagProcessing Descriptor

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |  Length       |            Vendor-Id          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Continuation |               TLV
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Type-ID	85 for VLANTagProcessing Descriptor
Description	This attribute describes the rules for the processing of the VLAN tags of an ETH packet flow. The VLANTagProcessing descriptor may be pre-provisioned.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	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.

TLD ID	1 for VLANTagProcessingRuleID
Description	ID of the particular rule
Length	2+2
Value	Unsigned-Short • 0x0000: reserved with special meaning

TLD ID	2 for C-VLAN Priority Setting
Description	Defines the setting of the priority_bits in the C-VLAN tag in the upstream direction.
Length	2+1
Value	Bitfield; the bits have the following meaning: • 0x00 = forward the p_bits without modification • 0x1x = drop frames with p_ bits set to a higher value than x • 0x2x = set p_bits to x when p_bits set to a higher value than x • 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. Other values reserved. Note: One of the bitfield definitions can be assigned at a time.

TLD ID	3 for VLAN ID Assignment
Length	2+2
Description	Defines the processing of the C-VLAN tag and S-VLAN tag

Value	Bitfield; the bits have the following meaning: • 0x0000 = forward VLAN tags without modification • 0x0010 = remove S-VID in downstream direction • 0x0020 = remove C-VID and S-VID, if present, in downstream direction • 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 • 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 • 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 • 0x040x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C->S-VID Mapping table and S-p_bits set to x If no entry exists for a particular C-VID in the C->S-VID Mapping table, the S-VID is set to 0 • 0x0480 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C->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->S-VID Mapping table, the S-VID is set to 0 Other values reserved. One downstream rule can be combined (ORed) with one upstream rule.

TLV ID	4 for SVLAN-ID
Description	The value of the field specifies the SVALN ID value for the Ethernet frame.
Length	2+2
Value	Only the lower 12 bits of the 2 byte value are significant; the upper four bits SHALL be ignored.

TLV ID	5 for CVLAN-ID
Description	The value of the field specifies the CVLAN-ID value for the Ethernet frame.
Length	2+2
Value	Only the lower 12 bits of the 2 byte value are significant; the upper four bits SHALL be ignored.

TLV ID	6 for C-VID>S-VID Mapping
Description	The value of the field specifies a mapping between a C-VID and a S-VID
Length	2+4
Value	C-VID,S-VID Only the lower 12 bits of the 2 byte VID values are significant; the upper four bits SHALL be ignored.

TLD ID	7 for LocalConfigInfo
Description	Local configuration information for preprovisioned R3 data path (Simple Ethernet)
Length	2+n
Value	String of length n containing arbitrary information The meaning of the information in LocalConfigInfo is subject of static configuration agreements between NAP and NSP.

5.4.3.90 hDHCP-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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |  Length       |           Vendor-Id           |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Continuation |               TLV
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	86 for hDHCP-Server-Parameters
Description	This attribute contains the Home DHCP server and corresponding security keys.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	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.

TLV ID	1 for DHCPv4-Server
Description	The IPv4 address of the home DHCP-Server to use for IPv4 address allocation by the ASN.
Length	2+4
Value	Octet string containing an IPv4 address (most significant bit first).

TLV ID	2 for DHCPv6-Server
Description	The IPv6 address of the home DHCP-Server to use for IPv6 allocation by the ASN.
Length	2+16
Value	Octet string containing an IPv6 address (most significant bit first).

TLV ID	3 for DHCP-RK
Description	The hDHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
Length	2 + 2(SALT) + length of the String containing the encrypted hDHCP-RK.
Value	The value consists of 2 octets for the SALT (see [48]) and a String containing the encrypted hDHCP-RK formulated as per [48].

TLV ID	4 for DHCP-RK-Key-ID
Description	An integer number uniquely identifying the hDHCP-RK within the scope of a single DHCP server.
Length	2 + 4
Value	Unsigned 32-bit integer MSB first.

TLV ID	5 for DHCP-RK-Lifetime
Description	Lifetime of the hDHCP-RK and derived keys.
Length	2 + 4
Value	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

5.4.3.91 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Vendor-Id (cont)           | WiMAX TYPE    |     Length    |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Continuation |               TLV
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	87 for vDHCP-Server-Parameters
Description	This attribute contains a Visited DHCPv4 server and corresponding security keys.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	AR
1	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.

TLV ID	1 for DHCPv4-Server
Description	The IPv4 address of the visited DHCP-Server to use for IPv4 address allocation by the ASN.
Length	2+4
Value	Octet string containing an IPv4 address (most significant bit first).

TLV ID	2 for DHCPv6-Server
Description	The IPv6 address of the home DHCP-Server to use for IPv6 allocation by the ASN.
Length	2+16
Value	Octet string containing an IPv6 address (most significant bit first).

TLV ID	3 for DHCP-RK
Description	The DHCP-RK generated by the AAA server that is sent to the NAS upon successful EAP authentication.
Length	2 + 2(SALT) + length of the String containing the encrypted vDHCP-RK.
Value	The value consists of 2 octets for the SALT (see [48]) and a String containing the

	encrypted hDHCP-RK formulated as per [48].

TLV ID	4 for DHCP-RK-Key-ID
Description	An integer number uniquely identifying the vDHCP-RK within the scope of a single DHCP server.
Length	2 + 4
Value	Unsigned 32-bit integer MSB first.

TLV ID	5 for DHCP-RK-Lifetime
Description	Lifetime of the DHCP-RK and derived keys.
Length	2 + 4
Value	Unsigned 32-bit integer MSB first representing the number of seconds the key is valid.

5.4.3.92 PMIP6-Service-Info

```
   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  |       PMIP6 service info      |
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	126 for PMIP6-Service-Info
Description	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.
Length	6 + 3 + 2
Continuation	C-bit = 0
Value	2 Octets Bitmask defined as follows: • Bit #0 = Mobility support for IPv6 • Bit #1 = Mobility support for IPv4 • Bit #2 = IPv4 transport backhaul support • Bit #3 = Lower-layer transport security • Bit #4 = In-band protocol security All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.4.3.93 hLMA-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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	127 for hLMA-IPv6-PMIP6
Description	The IPv6 address of the LMA in the HCSN assigned for the MS/AMS's PMIP6 session.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet-String representing an IPv6 address (the most significant octet first)

5.4.3.94 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	128 for hLMA-IPv4-PMIP6
Description	The IPv4 address of the LMA in the HCSN assigned for the MS/AMS's PMIP6 session.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet-String representing an IPv4 address (the most significant octet first)

5.4.3.95 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
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	129 for vLMA-IPv6-PMIP6
Description	The IPv6 address of the LMA in the VCSN assigned for the MS/AMS's PMIP6 session.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet-String representing an IPv6 address (the most significant octet first)

5.4.3.96 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	130 for vLMA-IPv4-PMIP6
Description	The IPv6 address of the LMA in the HCSN assigned for the MS/AMS's PMIP6 session.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet-String representing an IPv4 address (the most significant octet first)

5.4.3.97 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	131 for PMIP6-RK-KEY
Description	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.
Length	6 + 3 +2(SALT)+ Length of the encrypted PMIP6-RK-KEY
Continuation	C-bit = 0
Value	The value consists of 2 octets for the SALT (see [40]) and a String containing the encrypted PMIP6-RK-KEY formulated as per Section 4.3.1.1.

5.4.3.98 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	132 for PMIP6-RK-SPI
Description	The SPI associated with the PMIP6-RK-KEY
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer, MSB first.

5.4.3.99 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	133 for Home-HNP-PMIP6
Description	The IPv6 Home Network Prefix assigned by the AAA in HCSN to the MS/AMS for PMIP6 mobility session.
Length	6 + 3 + 1 + (0-16)
Continuation	C-bit = 0
Value	Octet string contains one byte of “Prefix-Length” and up to 16 bytes of Home Network Prefix

5.4.3.100 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	134 for Home-Interface-Id-PMIP6
Description	The IPv6 interface Id assigned by the HCSN to be used for PMIP6 address configuration via DHCPv6
Length	6 + 3 + 8
Continuation	C-bit = 0
Value	Octet string containing the IPv6 interface identifier (most significant bit first)

5.4.3.101 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
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	135 for Home-IPv4-HoA-PMIP6
Description	The IPv4 Home Address assigned by the HCSN to the MS/AMS for PMIP6-IPv4 mobility session.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing the IPv4 address (most significant bit first)

5.4.3.102 Visited-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 |          Visited-HNP
  +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	136 for Visited-HNP-PMIP6
Description	The IPv6 Home Network Prefix assigned by VCSN to the MS/AMS for PMIP6 mobility session.
Length	6 + 3 + 1 + (0-16)
Continuation	C-bit = 0
Value	Octet string contains one byte of “Prefix-Length” and up to 16 bytes of Home Network Prefix

5.4.3.103 Visited-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  |              Visited-Interface-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	137 for Visited-Interface-Id-PMIP6
Description	The IPv6 interface Id assigned by the VCSN to be used for PMIP6 address configuration via DHCPv6
Length	6 + 3 + 8
Continuation	C-bit = 0
Value	Octet string containing the IPv6 interface identifier (most significant bit first)

5.4.3.104 Visited-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 |        Visited-IPv4-HoA
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	138 for Visited-IPv4-HoA-PMIP6
Description	The IPv4 Home Address assigned by the VCSN to the MS/AMS for PMIP6-IPv4 mobility session.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing the IPv4 address (most significant bit first)

5.4.3.105 BS-Location

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|RADIUS TYPE 26 |   Length      |           Vendor-ID           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Vendor-ID (cont)             |   WiMAX TYPE  |    Length     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Continuation  |                   BS-Location
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	88 for BS-Location
Description	An alternative Serving BS/ABS identification information to BS-ID. Normally indicates the location information of the serving BS/ABS which may be described as Lat/Long/Sector/carrier information of the serving BS/ABS.
Length	6 + 3 + Length of Location (>0)
Continuation	C-bit = 0 or 1
Value	Octet string representing location. Format is 0.

5.4.3.106 Mobility-Access-Classifier

```
 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  |            Mobility-Access-Classifier
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	89 for Mobility-Access-Classifier
Description	In an Access-Accept the attribute identifies the classification of the subscriber at the H-AAA as a fixed, nomadic or mobile access subscriber.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	• 1 = Fixed • 2 = Nomadic • 3 = mobile 4-255= Reserved

5.4.3.107 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      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	90 for MS-Authenticated
Description	A flag indicating whether the MS/AMS has successfully performed device authentication during initial network entry or not.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Unsigned Octet. When set to (1) the MS/AMS 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.

5.4.3.108 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.)
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

<table>
<tr><td><b>WType-ID</b></td><td>126 for Operator-Name</td></tr>
<tr><td><b>Description</b></td><td>This attribute is defined in [97] and contains the country code and the WiMAX assigned company code of the role of the WiMAX operator.</td></tr>
<tr><td><b>Length</b></td><td>62 + 1 + 7</td></tr>
<tr><td><b>Value</b></td><td>The Text field is formatted as follows:
<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>
Where the Namespace ID is as defined by [97] with the value of 0x34 assigned by IANA to WiMAX.

The Operator-Name field is of type Text and is defined by this specification to consist of 3 sub-fields as follows:

The first sub-field consists of a single octet enumeration encoded in ASCII defining the role of the operator as follows:
• “0” (0x30) Reserved
• “1” (0x31) The operator role is a Visited NSP.
• “2” (0x32) The operator role is a Home NSP.
• All other values reserved.
The second sub-field consists of 3 octets encoded in ASCII representing the ISO 3166-1</td></tr>
</table>

	alpha-3 Country Code of the operator. The codes "WF1" and "WF2" SHALL be reserved for Marine and Satellite operators respectively by the WiMAX Forum. 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".

5.4.3.109 Certified-MS-Feature-List

```
  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 |            TLVs
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	140 for Certified-MS-Feature-List
Description	List of CVS feature packages for the MS/AMS that are relevant for the ASN policy for this MS/AMS. Upon receipt the ASN-GW will take appropriate action based on ASN policy for the feature packages where the ASN-GW acts as policy decision point. The ASN-GW will also forward the content to the BS/ABS across R4/R6. The AAA server MUST not include more than one instance of this attribute with an identical Feature-Package-List-Version value. If an ASN-GW receives this attribute/AVP with an unknown Feature-Package-List-Version, it SHALL ignore the Attribute/AVP. This document does not define any specific behavior upon receipt of the certified MS/AMS feature list and assumes this to be internal to the BS/ABS or ASN-GW.
Length	6 + 3 + TLVs
Continuation	C-bit = 0
Value	The attribute MUST contain one Feature-Package-List-Version TLV followed by one Feature-Package-List TLV where the feature package numbers defined by table A (ASN feature packages) in "Annex A: " are used.

TLV ID	TLV Name	Length Octets	AR	AA	AC	R
1	Feature-Package-List-Version	2+2	0	1	0	0
2	Feature-Package-List	2+Variable	0	1	0	0

TLV ID	1 for Feature-Package-List-Version
Description	The Version of the subsequent Feature-Package-List.
Length	2+2 octet
Value	The value is set to '1'.

TLV ID	2 for Feature-Package-List
Description	Indicates for each feature package whether the MS/AMS is certified or not.
Length	Variable (2 + roundup(n/8) where n is the number of bits that corresponds to the number of feature packages)
Value	The bitmap representing the list of feature packages. The bitmap is encoded as a bitstream where bit 0 is the most significant bit which is sent first (bit 0 of the first octet). Bit 8 of the bitstream is the first bit of the second octet etc. Each bit corresponds to the feature package number as defined by “Annex A: “. A value of ‘0’ means that the MS provided a IPID value during network entry which indicates that the MS is not certified for this feature package (or the feature package should not be enabled for this MS based on other reasons subject to the operator’s policy). The number of octets depends on the number of feature packages to be encoded as identified by the respective feature package table. Example: • Bit-#0 – reserved • Bit-#1 – Feature Package 1 (0 = not certified; 1 = certified) • Bit-#2 – Feature Package 2 (0 = not certified; 1 = certified) • Etc. All bits where no feature package corresponding to the bit number is defined, are reserved. All reserved bits MUST be set to ‘0’ by the sender and are ignored by the receiver.

5.4.3.110 Present-Authenticator-Verification-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 |            PA-VC
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	141 for Present-Authenticator-Verification-Code
Description	Present Authenticator Validation Code (MSK Hash1)
Length	6 + 3 + 32
Continuation	C-bit = 0
Value	MSK Hash1

5.4.3.111 OCR-Count

```
 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 |            OCR-Count (nonce1)
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	142 for OCR-Count
Description	Present Authenticator OCR_COUNT
Length	6 + 3 + 2
Continuation	C-bit = 0
Value	Nonce set by the present authenticator to the value of CMAC_KEY_COUNT

5.4.3.112 Local-Routing-Indication

```
 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 |      LRS      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	244 for Local-Routing-Indication
Description	Indicates whether the service is local routing enabled by ASN GW.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	Bitmap: - Bit #0 – Local Routing at ASN-GW All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits

5.4.3.113 Local-Routing-Indication

```
 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 |      LRS      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	245 for ALR-Command
Description	This attribute contains ALR command for obtaining/providing dynamic authorization.
Length	6 + 3 + TLV
Continuation	C-bit = 0 or 1
Value	The sub-types described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	ARj	COA	COA-ACK
1	Action	2+1	1	1	0	0	1	1
2	WiMAX-session-id-1	2+4	1	0	0	0	1	0
3	WiMAX-session-id-2	2+4	1	0	0	0	0-1	0
4	IPv6-address-1	2+16	0-1[a]	0	0	0	0-1[a]	0
5	IPv6-address-2	2+16	0-1[a]	0	0	0	0-1[a]	0
6	IPv4-address-1	2+4	0-1[a]	0	0	0	0-1[a]	0
7	IPv4-address-2	2+4	0-1[a]	0	0	0	0-1[a]	0

Notes:

[a] Either both of the IPv6-address-1 and IPv6-address-2, or both of the IPv4-address-1 and IPv4-address-2 TLVs shall be present in any packet, with one exception. Exception is the case when CoA is used for terminating ALR for all of the service flows associated with the given WiMAX session(s) in which case none of the IP address TLVs are included in the CoA packet.

TLV ID	1 for Action
Description	The code that indicates the requested action when used in AR and the result when used in AA.
Length	2+1 octet
Value	1 octet value defined as follows: •0 = Start. Used in request messages. •1 = Stop. Used in request messages.

	•2 = Accepted. Used in response messages. •3 = Rejected. Used in response messages. Other values reserved.

TLV ID	2 for WiMAX-session-id-1
Description	WiMAX session identifier for the service flow that is managed by the CSN (i.e., local to the CSN).
Length	2+4 octet
Value	Octet String. The value of the WiMAX-Session-Id.

TLV ID	3 for WiMAX-session-id-2
Description	WiMAX session identifier for the other service flow that is managed by the CSN (i.e., local to the CSN).
Length	2+4 octet
Value	Octet String. The value of the WiMAX-Session-Id.

TLV ID	4 for IPv6-address-1
Description	End-to-end flow that is subject to ALR has two end-points and hence two associated IP addresses. This is the IPv6 address that belongs to one of the end-points.
Length	2+16 octet
Value	Octet String. An IPv6 address.

TLV ID	5 for IPv6-address-2
Description	End-to-end flow that is subject to ALR has two end-points and hence two associated IP addresses. This is the IPv6 address that belongs to the other end-point.
Length	2+16 octet
Value	Octet String. An IPv6 address.

TLV ID	6 for IPv4-address-1
Description	End-to-end flow that is subject to ALR has two end-points and hence two associated IP addresses. This is the IPv4 address that belongs to one of the end-points
Length	2+4 octet
Value	Octet String. An IPv4 address.

TLV ID	7 for IPv4-address-2
Description	End-to-end flow that is subject to ALR has two end-points and hence two associated IP addresses. This is the IPv6 address that belongs to the other end-point.
Length	2+4 octet
Value	Octet String. An IPv4 address.

5.4.3.114 MCBCS-Controller-Server-IPv4

```
    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 |      MCBCS Controller/Server IPv4             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	106 for MCBCS-Controller-Server-IPv4
Description	MCBCS Controller/Server IPv4.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	The value of this AVP is encoded as an IPv4 address.

5.4.3.115 MCBCS-Controller-Server-FQDN

```
    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 |      MCBCS Controller/Server FQDN             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	107 for MCBCS-Controller-Server-FQDN
Description	Fully qualified domain name of the MCBCS Controller/Server for the given MCBCS service.
Length	6 + 3 + Length of FQDN of the MCBCS Controller/Server
Continuation	C-bit = 0
Value	Octet string containing a Domain Name (most significant octet first).

5.4.3.116 MCBCS-Controller-Server-IPv6

```
    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 |      MCBCS Controller/Server IPv6             |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	108 for MCBCS-Controller-Server-IPv6
Description	MCBCS Controller/Server IPv6.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	The value of this AVP is encoded as an IPv6 address.

5.4.3.117 MCBCS-Service-Association-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 |      MCBCS Service Association SPI            |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	109 for MCBCS-Service-Association-SPI
Description	Index a MCBCS Proxy service association with the MCBCS Controller/Server..
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Unsigned 32-bit integer MSB first.

5.4.3.118 MCBCS-Program-Descriptor

```
    0                   1                   2                   3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |RADIUS TYPE 26 |  Length       |            Vendor-Id          |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |    Vendor-Id (cont)           | WiMAX TYPE    |    Length     |
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
   |  Continuation |               TLV
   +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

WType-ID	110 for MCBCS-Program-Descriptor

Description	This attribute describes a MCBCS Program.
Length	6 + 3 + TLV
Continuation	C-bit = 0 or 1
Value	The sub-types are described below.

TLV ID	TLV Name	Length Octets	AR	AA	AC	ARj
1	MCBCS Program ID	2+2	0-1	1	0	0
2	MCBCS Transmission Zone ID	2+2	0-1	1	0	0
3	PDFID	2+2	0-n	1-n	0	0

TLV ID	1 for MCBCS Program ID
Description	The identifier of MCBCS Service package.
Length	2+2
Value	Unsigned Short representing the MCBCS Program identifier (most significant bit first). A value of zero(0) is invalid,

TLV ID	2 for MCBCS Transmission Zone ID
Description	The identifier of MCBCS Transmission Zone.
Length	2+ variable
Value	String

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.

To support Diameter extensions, the Diameter commands defined in this specification allow for the inclusion of any Diameter AVP as provided by the "*[AVP]" attribute in the commands' ABNF. The sender of these AVPs must not set the M-bit flag in the header of these AVPs thus allowing the receiver to silently discard attributes that it does not implement.

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 [55].

Application Abbrev	Application ID	Application Name	Description

WNAAADA	16777281	WiMAX® Network Access Authentication and Authorization Diameter Application	Application between the ASN and the AAA in the CSN.
WNADA	16777282	WiMAX® Network Accounting Diameter Application	Application between the ASN or HA and the AAA in the CSN
WM4DA	16777283	WiMAX® MIP4 Diameter Application	Application between the MIP4 HA and the AAA in the CSN for IPv4 mobility service.
WM6DA	16777284	WiMAX® MIP6 Diameter Application	Application between the MIP6 HA and the AAA in the CSN.
WDDA	16777285	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 (WNAADA) and WiMAX Network Accounting Diameter Application when performing the Capability Exchange procedure defined in RFC3588 [55].

A WiMAX compliant VAAA MUST advertise support for the WiMAX Network Access Authentication and Authorization Diameter Application (WNAADA) when performing the Capability Exchange procedure defined in RFC3588 [55].

A WiMAX compliant HA providing IPv4 mobility services MUST advertise support for the WiMAX MIP4 Diameter Application (WM4DA) and MAY advertise WiMAX Network Accounting Diameter Application when performing the Capability Exchange procedure defined in RFC3588 [55].

A WiMAX compliant HA providing IPv6 mobility services MUST advertise support for the WiMAX MIP6 Diameter Application (WM6DA) and MAY advertise WiMAX Network Accounting Diameter Application when performing the Capability Exchange procedure defined in RFC3588 [55].

A WiMAX compliant DHCP server MUST advertise support for the WiMAX DHCP Diameter Application (WDDA) when performing the Capability Exchange procedure defined in RFC3588 [55].

A WiMAX compliant HAAA MUST advertise support for the WiMAX Network Access Authentication and Authorization Diameter Application (WNAADA), WiMAX MIP4 Diameter Application (WM4DA) and WiMAX Network Accounting Diameter Application (WNADA) when performing the Capability Exchange procedure defined in RFC3588 [55]. The HAAA MAY advertise support for WiMAX MIP6 Diameter Application (WM6DA) and WiMAX DHCP Diameter Application (WDDA) when performing the Capability exchange procedure defined in RFC3588 [55].

When the Supported-Vendor-Id AVP is used, the value carried MUST be set to the WiMAX Forum's IANA-assigned SMI Network Management Private Enterprise Code (24757). The Vendor-Id AVP MUST be set to the equipment vendor's IANA-assigned SMI Network Management Private Enterprise Code.

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 [67]. 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 5-22 – Commands of WiMAX® Network Access Authentication and Authorization Diameter Application

Command-Name	Abbrev.	Code
WiMAX-Diameter-EAP-Request	WDER	8388609
WiMAX-Diameter-EAP-Answer	WDEA	8388609
WiMAX-Diameter-OCR-Request	WDOR	<IANA Pending>WDO
WiMAX-Diameter-OCR-Answer	WDOA	<IANA Pending>WDO
WiMAX-Change-of-Authorization-Request	WCAR	8388610
WiMAX-Change-of-Authorization-Answer	WCAA	8388610
WiMAX-Reauthentication-Request	WRAR	8388611
WiMAX-Reauthentication-Answer	WRAA	8388611
WiMAX-Session-Termination-Request	WSTR	8388612
WiMAX-Session-Termination-Answer	WSTA	8388612
WiMAX-Abort-Session-Request	WASR	8388613
WiMAX-Abort-Session-Answer	WASA	8388613

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 [67] 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: 8388609, 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 VNSP.
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]

Table of occurrence of WiMAX® VSAs in a DER command for initial authentication, that is, a DER command that has Auth-Request-Type set to AUTHORIZE_AUTHENTICATE and containing EAP Response(Identity).

Table 5-23 – 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.

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 5-24 – 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.

Table 5-25 – 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.

Table of WiMAX attribute for the DER Command.

Table 5-26 – 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 [75]		V
Calling-Station-Id	31	UTF8String	RFC4005 [63]	M	V
Operator-Name	126	UTF8String	[97]	M	V
WiMAX-Session-Id	4	OctetString		M,V	
GMT-Time-Zone-Offset	3	Unsigned32		M,V	

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must Not
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 [67] 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.

The WiMAX® Network Access and Authorization Diameter Application extends the DEA command by adding the following WiMAX AVPs:

Table 5-27 – WiMAX® Diameter-EAP-Answer (WDEA) Command

```
<WiMAX Diameter-EAP-Answer> ::= < Diameter Header: 8388609, PXY >
                                  * * * * * * * * * *
                                  [Chargeable-User-Identity]
```

[WiMAX-Capability]	
[WiMAX-Session-Id]	
* [Packet-Flow-Descriptor] [43]	
* [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]	
[Framed-IP-Address]	
[Framed-IPv6-Prefix]	
[Framed-Interface-Id]	
[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	

[43] This TLV is deprecated in this release and SHALL not be used. Only Packet Flow Descriptor V2 SHALL be used in this Release

[hDHCPv4-Server]	.
[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-Classifier]	

Feature Information

[Certified-MS-Feature-List-For-GW]
[Certified-MS-Feature-List-For-BS]
* [AVP]

The following table specifies the rules for including WiMAX VSAs in a DEA command when the Result-Code is set to DIAMETER_MULTI_ROUND_AUTH. This is equivalent to the RADIUS Access-Challenge packet.

Table 5-28 – 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-Classifier	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 5-29 – 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	0-n	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/AMS 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	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. 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. 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.
Visited-Framed-IPv6-Prefix	0-1	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. 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. 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
Visited-Framed-Interface-Id	0-1	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. 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. 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. If this attribute is included then Visite-Framed-IPv6-Prefix AVP MUST also be included.
hHA-IP-MIP4	0-1	The Home network MAY include an HA for the session in the home network by sending this parameter. At least hHA-IP-MIP4 or vHA-IP-MIP4 MUST be present in the DEA
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	SHALL be included if the Home network wants to assign an MIP6 HA in the home network. See vHA-IP-MIP6 note below.
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	0-1	
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 IPID is received as part of NAI decoration.
Certified-MS-Feature-List-For-BS	0	SHALL be present if IPID 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 [75], 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 DIAMTER 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 [55]). 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/AMS. As per [53] 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.

Table 5-30 – 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 [75]		V
Operator-Name	126	UTF8String	[97]	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	

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must Not
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	
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-Classifier	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	

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must Not
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® Diameter OCR Request/Answer Commands

The following describes only the WiMAX specific VSA that are being added to the WDOR and WDOA commands.

WiMAX® Diameter OCR Request (WDOR) Command

The WiMAX Diameter OCR Request Command is derived from the WDER Command and is used to carry out OCR authentication between the ASN and the CSN.

Following changes are applied on the WDER in order to define WDOR:

- EAP AVP is not carried in WDOR.
- Two new AVPs are carried in WDOR (namely, PA-VC and OCT-COUNT AVPs).

Other AVPs used in the WDOR are same as the ones used with a WDER whose Auth-Request-Type is set to AUTHENTICATE_ONLY.

```
<WiMAX Diameter-OCR-Request> ::= < Diameter Header: TBDWDOR , REQ, PXY >
                     * * * * * * * * * *            Attributes defined for WDER, except EAP
                                                    AVP.

                     [ PA-VC(MSKHash1) ]
                     [ OCR-COUNT ]
                     * [ AVP ]
```

Table 5-31 – Table of occurrence for AVPs in a WDOR command in terms of the differences with the WDER command.

Attribute	Occurrence	Notes
EAP	0	Shall not be carried in Diameter OCR commands.
PA-VC (MSKHash1)	1	
OCR-COUNT	1	

Table 5-32 – Attributes of the WDOR command in terms of the new ones with respect to the WDER command.

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must Not
PA-VC (MSKHash1)	141	OctetString		V	
OCT-COUNT	142	OctetString		V	

Note: V stands for Vendor Specific.

WiMAX® Diameter OCR Answer (WDOA) Command

The WiMAX Diameter OCR Answer Command is derived from the WDEA Command and is used to carry out OCR authentication between the ASN and the CSN. The only difference between the WDER and WDOA is that the latter does not carry EAP AVP. All the other details are the same (see 5.5.1.1.1)

5.5.1.1.3 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 8388610, 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:

Table 5-33 – WiMAX® Change-of-Authorization-Request Command

```
<WCA-Request> ::= < Diameter Header: 8388610, 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 5-34 – 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	-
IP-Redirection-Rule	55	Grouped	-	M,V	-
Hotline-Session-Timer	56	Unsigned32	-	M,V	-
Hotline-Indication	24	UTF8String	-	M,V	-

WiMAX® Change-of-Authorization-Answer Command

The WiMAX Change-of-Authorization-Answer (WCAA) command, indicated by the Command-Code field set to 8388610, is sent from the NAS or the HA to the AAA in order to report the result of the WCAR command.

The WCAA message format is defined as follows:

<WCA-Answer> ::= < Diameter Header: 8388610, 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]

Table 5-35 – 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
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

5.5.1.1.4 WiMAX® Reauthentication Request/Answer Command

This specification extends the Reauthentication-Request/Answer Command as defined in RFC3588 [55] 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 [75], was completed after RFC3588 [55] 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: 8388611, 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]

Table 5-36 – 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

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
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

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 includes 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: 8388611, PXY >

                                    < Session-Id >
```

```
{ Result-Code }
{ Origin-Host }
{ Origin-Realm }
{ Auth-Application-Id }
{ WiMAX-Session-Id }
[ 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 ]
```

Table 5-37 – 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
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

The AAA client MUST includes the Chargeable-User-Identity AVP in a WRAA command, if it knows the Chargeable-User-Identity (if it received it in a DEA or other means such as a context transfer for this session); in this case, the M-bit of the Chargeable-User-Identity AVP MUST be set. Otherwise, the Chargeable-User-Identity AVP MUST NOT be included in the WRAA command.

5.5.1.1.5 WiMAX® Session Termination Request/Answer Command

This specification extends the Session Termination Request/Answer commands as defined in RFC3588 [55] 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 [75], was completed after RFC3588 [55] was published.

WiMAX® Session Termination Request (WSTR) command

The WiMAX Session Termination Request command (WSTR) is sent from the ASN to the AAA server in the CSN to advice that WiMAX session is terminating at that ASN (for example, due to Anchor Authenticator relocation) or terminating in entirely, due to network exit procedure.

WiMAX Session Termination Request (WSTR) command definition follows:

```
<WST-Request> ::= < Diameter Header: 8388612, REQ, PXY >
                  < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                  { Destination-Realm }
                  { Auth-Application-Id }
                  { 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 5-38 – 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

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
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: 8388612, 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 5-39 – 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
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

5.5.1.1.6 WiMAX® Abort Session Request/Answer Command

This specification extends the Abort Session Request/Answer commands as defined in RFC3588 [55] 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 [75], was completed after RFC3588 [55] 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: 8388613, 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]

Table 5-40 – 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
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

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
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

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® 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: 8388613, PXY >
                  < Session-Id >
                  { Result-Code }
                  { Origin-Host }
                  { Origin-Realm }
                  { Auth-Application-Id }
                  { 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 5-41 – 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
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 [62].

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	8388614
WiMAX-Home-Agent-IPv4-Answer	WHA4A	8388614
WiMAX-Change-of-Authorization-Request	WCAR	8388610
WiMAX-Change-of-Authorization-Answer	WCAA	8388610
WiMAX-Session-Termination-Request	WSTR	8388612
WiMAX-Session-Termination-Answer	WSTA	8388612
WiMAX-Abort-Session-Request	WASR	8388613
WiMAX-Abort-Session-Answer	WASA	8388613

The following commands are reused from the WiMAX Network Access Authentication and Authorization Diameter Application. The Auth-Application-Id AVP in these commands MUST be set to 16777283.

- 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: 8388614, 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 [55]
{ 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 5-42 – 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
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

WiMAX-Home-Agent-IPv4-Answer (WHA4A) Command

This command is sent by the AAA to the HA in response to a WMHAR command. The following specifies the allowed AVP in the command:

<WHA4A> ::= < Diameter Header: 8388614, 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

2 **Table 5-43 – 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	

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
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	
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 [85].

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	8388615
WiMAX-Home-Agent-IPv6-Answer	WHA6A	8388615
WiMAX-Change-of-Authorization-Request	WCAR	8388610
WiMAX-Change-of-Authorization-Answer	WCAA	8388610
WiMAX-Session-Termination-Request	WSTR	8388612
WiMAX-Session-Termination-Answer	WSTA	8388612
WiMAX-Abort-Session-Request	WASR	8388613
WiMAX-Abort-Session-Answer	WASA	8388613

The following commands are reused from the WiMAX Network Access Authentication and Authorization Diameter Application (see Table 5-22). The Auth-Application-Id AVP in these commands MUST be set to 16777284.

- 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: 8388615,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 [55]
{ 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 5-44 – 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: 8388615, 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]	

Table 5-45 – 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

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
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
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 [55].

Messages exchanged as part of the WiMAX DHCP Diameter Application MUST have their Auth-Application-Id AVP set to 16777285.

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	8388616
WiMAX-DHCP-Answer.	WDHCPA	8388616

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: 8388616, 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 [55]
{ 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 5-46 – Attributes of the WDHCPR 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 WDHCPR command.

```
< WDHCPA > ::= < Diameter Header: 8388616, 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 WDHCPR 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 5-47 – 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

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
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 [64] and modified in TS32.299 [100]. 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 [55].

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 [55]).

The termination of the Diameter user session is specified in RFC 3588 [55]. 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 [55]) 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 ]
```

Table 5-48 illustrates the basic structure of Diameter Credit Control Credit-Control-Request message as used for Online Charging.

Table 5-48 – 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_C	This field contains the destination peer address of the OCS identity.
User-Name	O_C	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_C	
Origin-State-Id	O_C	This field contains the state associated to the Charging Trigger Function (CTF).
Event-Timestamp	O_C	This field corresponds to the exact time the quota is requested.
Subscription-Id	O_M	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_C	Not used in WiMAX.
Termination-Cause	O_C	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_C	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_M	This field indicates whether the CTF is capable of handling multiple services independently.
Multiple-Services-Credit Control	O_C	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_C	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_C	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_C	This field contains the requested amount of octets to be sent and received.
CC-Input-Octets	O_C	This field contains the requested amount of octets to be received.
CC-Output-Octets	O_C	This field contains the requested amount of octets to be sent.
CC-Service-Specific-Units	O_C	This field contains the requested amount of service specific units, e.g. number of events.
AVP	O_C	
Used-Service-Unit	O_C	This field contains the amount of used non-monetary service units measured for a particular category to a particular quota type.
Reporting-Reason	O_C	
Tariff-Change-Usage	O_C	This field identifies the reporting period for the used service unit, i.e. before, after or during tariff change.
CC-Time	O_C	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_C	This field contains the amount of sent and received octets.
CC-Input-Octets	O_C	This field contains the amount of received octets.
CC-Output-Octets	O_C	This field contains the amount of sent octets.
CC-Service-Specific-Units	O_C	This field contains the amount of service specific units, e.g. number of events.
AVP	O_C	
Tariff-Change-Usage	-	Not used in CCR.
Service-Identifier	O_C	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_C	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_C	
Time-Quota-Type	M	
Trigger	O_C	Used as defined in [100].
Trigger-Type	O_C	Used as defined in [100].
AVP	O_C	
Service-Parameter-Info	-	Not used in WiMAX.
Service-Parameter-Type	-	
Service-Parameter-Value	-	
CC-Correlation-Id	-	Not used in WiMAX.
User-Equipment-Info	O_C	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_C	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_C	This field contains an identifier inserted by a relaying or proxying node to identify the node it received the message from.
Service-Information	O_M	This parameter holds the individual service specific parameters.

WiMAX-Information	O_C	This parameter holds the WiMAX specific parameters.
R3-OC-Session-Continue	O_M	
Old-Session-Id	O_C	Included if initial Credit Request corresponds to an existing session.
Hotlining-Capabilities	O_C	
Framed-IP-Address	O_C	The IPv4 address allocated for the user
Framed-IPv6-Prefix	O_C	The IPv6 address prefix allocated for the user.
Access-Network-Charging-Identifier-Gx	O_C	
~~AF-Charging-Identifier~~	~~O_C~~	Only used in case of PCC. See [3] for further details.
Offline-Charging	O_C	
AVP	O_C	

Note: See TS32.240-720 [101] for the meaning of "OM" and "OC".

5.5.1.5.4 Credit-Control-Answer message

The Credit-Control-Answer message (CCA) is indicated by the command-code field being set to 272 and the 'R' bit being cleared in the Command Flags field. It is used between the credit-control server and the Diameter credit-control client to acknowledge a Credit-Control-Request command.

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 5-49 illustrates the basic structure of a Diameter Credit-Control-Answer message as used for online charging.

Table 5-49 – 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_C	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.

AVP	Category	Description
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	-	
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_C	This field contains all parameters for the CTF quota management and defines the quotas to allow traffic to flow.
Granted-Service-Unit	O_C	This field contains the amount of granted service units for a particular category.
Tariff-Time-Change	O_C	This field identifies the reporting period for the granted service units, i.e. before, after or during tariff change.
CC-Time	O_C	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_C	This field contains the amount for sent and received octets.
CC-Input-Octets	O_C	This field contains the amount for received octets.
CC-Output-Octets	O_C	This field contains the amount for sent octets.
CC-Service-Specific-Units	O_C	This field contains the amount for service specific units, e.g. number of events.
AVP	-	
Requested-Service-Unit	-	Not used in CCA.

AVP	Category	Description
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	-	
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_C	This field identifies the reporting period for the used service unit, i.e. before, after or during tariff change.
Service-Identifier	O_C	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_C	This field contains the identifier of a rating group.
G-S-U-Pool-Reference	O_C	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 [64].
Value-Digits	M	Used as defined in [64].

AVP	Category	Description
Exponent	O_C	Used as defined in [64].
Validity-Time	O_C	This field defines the time in order to limit the validity of the granted quota for a given category instance.
Result-Code	O_C	This field contains the result of the query.
Final-Unit-Indication	O_C	This field indicates that the Granted-Service-Unit containing the final units for the service.
Final-Unit-Action	O_C	This field indicates to the credit-control client the action to be taken when the user's account cannot cover the service cost.
Restriction-Filter-Rule	O_C	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_C	This field contains the name of the filter list for this user.
Redirect-Server	O_C	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_C	
Volume-Quota-Threshold	O_C	Used as defined in [100].
Unit-Quota-Threshold	O_C	Used as defined in [100].
Quota-Holding-Time	O_C	
Quota-Consumption-Time	O_C	
Trigger	O_C	Used as defined in [100].
Trigger-Type	O_C	Used as defined in [100].
AVP	-	
Cost-Information	O_C	Used as defined in [64].
Unit-Value	M	Used as defined in [64].
Value-Digits	M	Used as defined in [64].
Exponent	O_C	Used as defined in [64].
Currency-Code	M	Used as defined in [64].
Cost-Unit	O_C	Used as defined in [64].
Low-Balance-Indication	O_C	This field indicates whether the subscriber account balance went below a designated threshold set by his account.
Remaining-Balance	O_C	This field contains the remaining balance of the subscriber.

AVP	Category	Description
Unit-Value	M	Used as defined in [64].
Value-Digits	M	Used as defined in [64].
Exponent	O_C	Used as defined in [64].
Currency-Code	M	Used as defined in [64].
Final-Unit-Indication	- O_C	This field indicates that the Granted-Service-Unit containing the final units for the service.
Final-Unit-Action	O_C	This field indicates to the credit-control client the action to be taken when the user's account cannot cover the service cost.
Restriction-Filter-Rule	O_C	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_C	This field contains the name of the filter list for this user.
Redirect-Server	O_C	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.
Check-Balance-Result	O_C	This field contains the balance checking result.
Credit-Control-Failure-Handling	O_C	Used as defined in [64].
Direct-Debiting-Failure-Handling	O_C	Used as defined in [64].
Validity-Time	-	Not used in WiMAX.
Redirect-Host	O_C	This field defines the time in order to limit the validity of the granted quota for a given category instance.
Redirect-Host-Usage	O_C	Used as defined in [55].
Redirect-Max-Cache-Time	O_C	Used as defined in [55].
Proxy-Info	O_C	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_C	This field contains an identifier inserted by a relaying or proxying node to identify the node it received the message from.
Failed-AVP	O_C	
Service-Information	O_C	This parameter holds the individual service specific parameters.
WiMAX-Information	O_C	This parameter holds the WiMAX specific

AVP	Category	Description
		parameters.
R3-OC-Session-Continue	O_M	
AVP	O_C	

Note: See TS32.240-720 [101] for the meaning of "OM" and "OC".

5.5.1.5.5 R3-OC specific AVPs

R3-OC is based on RFC4006 [64]. 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 5-50.

Table 5-50 –R3-OC specific AVPs

				AVP Flag rules (note 1)	
Attribute Name	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 [55]. NOTE 2: The value types are defined in RFC 3588 [55].					

5.5.1.5.6 R3-OC Re-Used AVPs of external organizations

Table 5-51 lists the Diameter AVPs re-used by R3-OC interface from RFC4006 [64] and TS32.299 [100]. The other reused AVPs from the Diameter base protocol are not listed in Table 5-51.

Table 5-51 –R3-OC re-used Diameter AVPs

AVP	Reference	Description	Msg. Type
Access-Network-Charging-Identifier-Gx	[99]	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	[55]	This field identifis the Diameter Online application.	Both
CC-Input-Octets	[64]	This field contains the requested amount of octets to be received.	Both

CC-Output-Octets	[64]	This field contains the requested amount of octets to be sent.	Both
CC-Request-Type	[64]	This field defines the transfer type: event for event based charging and initial, update, terminate for session based charging.	Both
CC-Request-Number	[64]	This field contains the sequence number of the transferred messages.	Both
CC-Session-Failover	[64]	This field indicates if failover is supported.	CCA
CC-Service-Specific-Units	[64]	This field contains the requested amount of service specific units, e.g. number of events.	Both
CC-Time	[64]	This field contains the amount of requested time.	Both
CC-Total-Octets	[64]	This field contains the requested amount of octets to be sent and received.	Both
CC-Unit-Type	[64]	This field contains the type of units considered to be pooled.	CCA
Check-Balance-Result	[64]	This field contains the balance checking result.	CCA
Credit-Control-Failure-Handling	[64]	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	[64]	This field contains the cost information of a service, which the credit-control client can transfer transparently to the end user.	CCA
Cost-Unit	[64]	This field contains the unit of the Cost-Information as human readable string.	CCA
Currency-Code	[64]	This field identifies the currency.	CCA
Destination-Host	[55]	This field contains the destination peer address of the OCS identity.	CCR
Direct-Debiting-Failure-Handling	[64]	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	[55]	This field corresponds to the exact time the quota is requested	CCR
Exponent	[64]	This field contains the exponent value to be applied to Value-Digit-AVP.	CCA
Filter-Id	[63]	This field contains the name of the filter list for this user.	CCA
Final-Unit-Action	[64]	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	[64]	This field indicates that the Granted-Service-Unit containing the final units for the service.	CCA

Framed-IP-Address	[64]	The IPv4 address allocated for the user	Both
Framed-IPv6-Prefix	[64]	The IPv6 address prefix allocated for the user. The encoding of the value within this Octet String type AVP SHALL be as defined in [46], Clause 2.3. The "Reserved", "Prefix-Length" and "Prefix" fields SHALL be included in this order.	Both
Granted-Service-Unit	[64]	This field contains the amount of granted service units for a particular category.	CCA
G-S-U-Pool-Identifier	[100]	This field identifies a credit pool within the session.	CCA
G-S-U-Pool-Reference	[64]	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	[64]	This field indicates whether the CTF is capable of handling multiple services independently.	Both
Offline-Charging	[100]	This filed contains a reference to the Offline Charging.	CCR
Origin-Host	[55]	This field identifies the endpoint of the originated Diameter message.	Both
Origin-Realm	[55]	This field contains the Realm of the originator of any Diameter message.	Both
Origin-State-Id	[55]		CCR
Proxy-Host	[55]	This field contains the identity of the host that added the Proxy-Info.	Both
Proxy-Info	[55]		Both
Proxy-State	[55]	This field contains local state information.	Both
Quota-Consumption-Time	[100]	This field tains an idle traffic threshold time in seconds.	CCA
Quota-Holding-Time	[100]	This field contains the quota holding time in seconds.	CCA
Rating-Group	[64]	This field contains the identifier of a rating group.	Both
Redirect-Address-Type	[64]	This field defines the address type of the address given tin the Redirect-Server-Address field.	CCA
Redirect-Host	[55]	This field identifies the host where the message should be forwarded to.	CCA

Redirect-Host-Usage	[55]	This field dictates how the routing entry resulting from the Redirect-Host is to be used.	CCA
Redirect-Max-Cache-Time	[55]	This field contains the maximum number of seconds the peer and route table entries.	CCA
Redirect-Server	[64]	This field contains the address information of the redirect server.	CCA
Redirect-Server-Address	[64]	This field defines the address of the redirect server.	CCA
Remaining-Balance		This field contains the remaining balance of the subscriber.	CCA
Reporting-Reason	[100]	This field specifies the reason for usage reporting for one or more types of quota for a particular category.	CCR
Requested-Action	[64]	The field defines the type of action if the CC-Request-Type indicates EVENT.	CCR
Requested-Service-Unit	[64]	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 [64].	CCR
Restriction-Filter-Rule	[64]	This field provides filter rules corresponding to services that are to remain accessible.	CCA
Result-Code	[64]	This field contains the result of the query.	CCA
Route-Record	[55]		Both
Service-Context-Id	[64]	This field contains a unique identifier of the Diameter credit-control service specific document that applies to the request.	CCR
Service-Identifier	[64]	This field contains identity of the used service. This ID with the Service-Context-ID together forms an unique identification of the service.	Both
Session-Id	[55]	This field is used to identify a specific session.	Both
Subscription-Id	[64]	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	[64]	This field contains the user data content e.g. NAI for WiMAX.	CCR
Subscription-Id-Type	[64]	This field determines the type of the identifier, e.g. END_USER_NAI for WiMAX.	CCR
Tariff-Change-Usage	[64]	This field identifies the reporting period for the used service unit, i.e. before, after or during tariff change.	Both
Tariff-Time-Change	[64]	This field identifies the reporting period for the granted service units, i.e. before, after or during tariff change.	CCA

Termination-Cause	[55]	This field indicate the reason why a session was terminated.	CCR
Time-Quota-Mechanism	[100]		CCR
Time-Quota-Threshold	[100]	This field contains a threshold value in seconds.	CCA
Time-Quota-Type	[100]	This field indicate which time quota consumption mechanism SHALL be used for the associated Rating Group.	Both
Trigger	[100]	This field contains Trigger-Type.	Both
Trigger-Type	[100]	This field is used to negotiate triggers and when associated quota need to be re-authorised.	Both
Unit-Quota-Threshold	[100]	This field contains a threshold value in service specific units.	CCA
Unit-Value	[64]	This field specifies the units as decimal value.	CCA
User-Equipment-Info	[64]	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	[64]	This field determines the type of the identifier.	CCR
User-Equipment-Info-Value	[64]	This field contains the user MAC.	CCR
User-Name	[55]	This field contains the User-Name, in a format consistent with the NAI specification.	CCR
Used-Service-Unit	[64]	This field contains the amount of used non-monetary service units measured for a particular category to a particular quota type.	CCR
Value-Digits	[64]	This field contains the significant digits of the number.	CCA
Validity-Time	[64]	This field defines the time in order to limit the validity of the granted quota for a given category instance.	CCA
Volume-Quota-Threshold	[100]	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 4.4.3.3.7]. 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 ]
    [ Network-Technology ]
    [ Hotline-Indication ]
    [ Prepaid-Indicator ]
    [ Idle-Mode-Transition ]
    [ Local-Routing-Indication ]
    [ 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 5-52 provides the list of IETF Reused AVPs.

Table 5-52 – 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	Unsinged32	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	126	UTF8String	[97]	M	V

3GPP reused AVPs are listed in Table 5-53.

Table 5-53 – 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 5-54.

Table 5-54 – WiMAX® Specific AVPs

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				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	-

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
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	-
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	[100]	V,M	-
Trigger-Type	870	Enumerated	[100]	V,M	-
Unit-Quota-Threshold	1226	Unsigned32	[100]	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	-

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules	
				Must	Must not
Visited-Framed-Interface-Id	81	Unsigned64	5.5.2.62	V,M	-
Volume-Quota-Threshold	869	Unsigned32	[100]	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	-
Local-Routing-Indication	244	Unsigned32	5.5.2.187	V,M	-

5.5.1.6.4 AVP Occurrence Table

Table 5-55 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 5-55 – 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
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

AVP Name	Accounting mode		Accounting-Request			Accounting-Answer		
	IP	PD flow	START	INTERI M	STOP	START	INTERI M	STOP
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	0-1	0	0	0-1
Accounting-Input-Octets	X	X	0	1-2[17]	1-2[17]	0	0	0
Accounting-Input-Packets	X	X	0	1-2[17]	1-2[17]	0	0	0
Accounting-Output-Octets	X	X	0	1-2[17]	1-2[17]	0	0	0
Accounting-Output-Packets	X	X	0	1-2[17]	1-2[17]	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+
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
Network-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

AVP Name	Accounting mode		Accounting-Request			Accounting-Answer		
	IP	PD flow	START	INTERI M	STOP	START	INTERI M	STOP
Local-Routing-Indication	X	X	0-1[18]	0-1[18]	0-1[18]	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
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

AVP Name	Accounting mode		Accounting-Request			Accounting-Answer		
	IP	PD flow	START	INTERIM	STOP	START	INTERIM	STOP
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

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.

[17] If Accounting AVP are present twice, it indicates the first one is for the normal traffic, and the second one is for the local-routed traffic.

[18] If included, two sets of accounting counters (Accounting-Input-Octets, Accounting-Input-Packets, Accounting-Output-Octets, Accounting-Output-Packets) may be contained in a given stop and interim Accounting message where the first one is for normal traffic and the second one is for local-routed traffic. If only one set of accounting counters is present, it is for the normal traffic by default.

5.5.2 WiMAX® DIAMETER VSAs Definitions

The following section defines the WiMAX Vendors specific AVPs.

Value types are as specified by RFC3588 [55]. Bit-Map types are as specified in the RADIUS section [5.4.3]

5.5.2.1 WiMAX®-Capability

WType-ID	1 for WiMAX-Capability
Description	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.
Value-Type	Grouped
Value	

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] Note: MUST be included when the sender is an ASN-GW.

[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]

[Packet-Flow-Operation-Policy]

[Local-Routing-Support]

*[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
466	Packet-Flow-Operation-Policy	0-1[j]	0
469	Local-Routing-Support	0-1[k]	0

Notes:

[a] The absence of this AVP in a Request means that the HA does not support Hot-Lining. This attribute MUST be included when the Request is coming from an ASN-GW.

[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.

[j] This attribute is present when the serving ASN support the Packet Flow Operation Policy capability that is used to indicate the assigned policy for each packet flow. The “absence” of the Packet-Flow-Operation-Policy indicates the SF airlink encryption on/off capability is not supported by the ASN, and the airlink

encryption for the given service flow is a local implementation policy of the ASN.

[k] This attribute is present when the serving ASN support the SF-based Local Routing capability.

5.5.2.2 Device-Authentication-Indicator

WType-ID	2 for Device-Authentication-Indicator
Description	This attribute is deprecated in RADIUS and DIAMETER and MUST NOT be used.
Value-Type	
Value	

5.5.2.3 GMT-Time-Zone-Offset

WType-ID	3 for GMT-Timezone-offset
Description	The current offset in seconds of the local time at the NAS with respect to GMT time.
Value-Type	Integer32
Value	Indicating a timeoffset in seconds.

5.5.2.4 WiMAX®-Session-Id

WType-ID	4 for WiMAX-Session-Id
Description	A unique per realm identifier assigned to the WiMAX session by the Home network during network entry. The NAI contained in the User-Name and the WiMAX-Session-Id forms a unique identifier of the session at the NAS. 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.
Value-Type	OctetString
Value	Octet String. The value of the WiMAX-Session-Id

5.5.2.5 MSK

WType-ID	5 for MSK
Description	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.
Value-Type	OctetString
Value	Octet String. The value of the MSK.

5.5.2.6 hHA-IP-MIP4

WType-ID	6 for hHA-IP-MIP4
Description	The IPv4 address of the HA.
Value-Type	Address

Value	An IPv4 address as defined byRFC3588

5.5.2.7 hHA-IP-MIP6

WType-ID	7 for hHA-IP-MIP6
Description	The IPv6 address of the HA used for MIP6.
Value-Type	Address
Value	An IPv6 address as defined byRFC3588

5.5.2.8 hDHCPv4-Server

WType-ID	8 for DHCPv4-Server
Description	The IPv4 address of the DHCP-Server to use for IPv4 address allocation by the ASN.
Value-Type	Address
Value	IPv4 as defined by RFC3588

5.5.2.9 hDHCPv6-Server

WType-ID	9 for DHCPv6-Server
Description	The IPv6 address of the DHCP-Server to use for IPv6 allocation by the ASN.
Value-Type	Address
Value	IPv6 as defined by RFC3588

5.5.2.10 MN-HA-MIP4-KEY

WType-ID	10 for MN-HA-MIP4-KEY
Description	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.

5.5.2.11 MN-HA-MIP4-SPI

WType-ID	11 MN-HA-MIP4-SPI
Description	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.

5.5.2.12 MN-HA-MIP6-KEY

WType-ID	12 for MN-HA-MIP6-KEY
Description	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.

5.5.2.13 MN-HA-MIP6-SPI

WType-ID	13 MN-HA-MIP6-SPI
Description	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.

5.5.2.14 FA-RK-KEY

WType-ID	14 for FA-RK-KEY
Description	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.

5.5.2.15 HA-RK-KEY

WType-ID	15 for HA-RK-KEY
Description	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.

5.5.2.16 HA-RK-SPI

WType-ID	16 for HA-RK-SPI
Description	The SPI used for the HA-RK.
Value-Type	Unsigned32
Value	An unsigned value representing a SPI.

5.5.2.17 HA-RK-Lifetime

WType-ID	17 for HA-RK-Lifetime
Description	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

WType-ID	18 for RRQ-HA-IP
Description	The IPv4 or IPv6 address of the HA as contained in the MIP Registration Request or the BU.
Value-Type	Address
Value	Octet string containing an IPv4 or IPv6 address (most significant bit first)

5.5.2.19 RRQ-MN-HA-KEY

WType-ID	19 for RRQ-MN-HA-KEY
Description	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.
Value-Type	OctetString
Value	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].

WType-ID	21 for Session-Continue
Description	This attribute when set to ‘true’ means it is not the end of a Session and an Accounting Stop is immediately followed by an Account Start Record. ‘False’ means end of a session.

Value-Type	Enumerated
Value	Allowed values: • False(0) • True(1) All other values reserved

5.5.2.21 Beginning-of-Session

Note: This AVP is referenced by the PCC specification [3].

WType-ID	22 for Beginning-of-Session
Description	This attribute when set to 'true' means that this Accounting Start packet marks the start of a new flow. If set to 'False', this Accounting Start message is a continuation of a previous flow.
Value-Type	Enumerated
Value	Allowed values: • False(0) • True(1) All other values reserved

5.5.2.22 Network-Technology

Note: This AVP is referenced by the PCC specification [3].

WType-ID	23 for Network-Technology
Description	This attribute indicates which type of WiMAX session is being used.
Value-Type	Enumerated
Value	The enumeration is defined as follows: • 0 = Simple IPv4 • 1 = Simple IPv6 • 2 = PMIP4 • 3 = CMIP4 • 4 = CMIP6 • 5 = Ethernet-CS • 6 = Simple ETH • 7 = MIP based ETH All other values reserved

5.5.2.23 Hotline-Indication

Note: This AVP is referenced by the PCC specification [3].

WType-ID	24 for Hotline-Indication
Description	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.
Value-Type	UTF8String
Value	A string value which is to be opaque.

5.5.2.24 Prepaid-Indicator

Note: This AVP is referenced by the PCC specification [3].

WType-ID	25 for Prepaid-Indicator
Description	This attribute appears in Accounting messages and indicates to the backoffice that this session was associated with a prepaid user (on-line accounting). If the attribute is not present the session is deemed to be an offline (not prepaid) session.
Value-Type	Enumerated
Value	Allowed values: • Offline(0) • Online(1) All other values reserved

5.5.2.25 PDFID

WType-ID	26 for PDFID
Description	This value of this attribute matches all records from the same packet data flow. PDFID is assigned by the CSN and remains constant through all handover scenarios.
Value-Type	Unsigned32 (but not to exceed a range of 16 bits)
Value	Packet Data Flow Identifier. (Most significant bit first) less than 2^16

5.5.2.26 SDFID

WType-ID	27 for SDFID
Description	The value of this attribute matches all packet data flows from the same service data flow. SDFID is assigned by the CSN and remains constant through all handover scenarios.
Value-Type	Unsigned32 (but not to exceed a range of 16 bits)
Value	Service Data Flow Identifier (Most significant bit first) less than 2^16

5.5.2.27 Packet-Flow-Descriptor[44] (This AVP is deprecated in this release)

5.5.2.28 QoS-Descriptor

Type-ID	29 for QoS-Descriptor
Description	This attribute describes QoS parameters that are associated with a flow.

[44] This Attribute SHALL not be used, as the support of Packet Flow Descriptor is depricated in this release. Only Packet Flow Descriptor V2 SHALL be supported instead

Value-Type	Grouped

```
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 ]
                  [ Transmission-Policy ]
                  [DSCP]
                  [ Priority-Indication ]
                  * [ 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 5-54 If omitted the traffic priority is assumed to be 0.
317	Maximum-Sustained-Traffic-Rate	0-1	See Table 5-54
318	Minimum-Reserved-Traffic-Rate	0-1	See Table 5-54

TLV ID	TLV Name	Answer	Notes
319	Maximum-Traffic-Burst	0-1	See Table 5-54
320	Tolerated-Jitter	0-1	See Table 5-54
321	Maximum-Latency	0-1	See Table 5-54
322	Reduced-Resource-Code	0-1	See Table 5-54
323	Media-Flow-Type	0-1	See Table 5-54
325	Unsolicited-Grant-Interval	0-1	See Table 5-54
326	SDU-Size	0-1	See Table 5-54
327	Unsolicited-Polling-Interval	0-1	See Table 5-54
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	
465	Priority-Indication	0-1	Needed for ETS support

1 **Table 5-56 – 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]
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]

2 **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.

5.5.2.29 Control-Packets-In

Note: This AVP is referenced by the PCC specification [3].

WType-ID	31 for Control-Packets-In
Description	Packet counts for incoming Mobile IP, DHCP, ICMP messages for IPv4 and IPv6.
Value-Type	6 + 3 + 4
Value	Unsigned Integer representing packets count.

5.5.2.30 Control-Octets-In

Note: This AVP is referenced by the PCC specification [3].

WType-ID	32 for Control-Octets-In
Description	Octet counts for incoming Mobile IPv4, DHCP, ICMP messages etc.
Value-Type	6 + 3 + 4
Value	Unsigned Integer representing octets.

5.5.2.31 Control-Packets-Out

Note: This AVP is referenced by the PCC specification [3].

WType-ID	33 for Control-Packets-Out
Description	Packet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
Value-Type	6 + 3 + 4
Value	Unsigned Integer representing packets count.

5.5.2.32 Control-Octets-Out

Note: This AVP is referenced by the PCC specification [3].

WType-ID	34 for Control-Octets-Out
Description	Octet counts for outgoing Mobile IPv4, DHCP, ICMP messages etc.
Value-Type	6 + 3 + 4
Value	Unsigned Integer representing an octet count.

5.5.2.33 Active-Time

Note: This AVP is referenced by the PCC specification [3].

WType-ID	39 for Active-Time

Description	The amount of time the session was not in Idle state.
Value-Type	Unsigned32
Value	Unsigned Integer. The time in seconds.

5.5.2.34 DHCP-RK

WType-ID	40 for DHCP-RK
Description	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.
Value-Type	OctetString
Value	Key MSB first.

5.5.2.35 DHCP-RK-Key-ID

WType-ID	41 for DHCP-RK-Key-ID
Description	An integer number uniquely identifying the DHCP-RK within the scope of a single DHCP server.
Value-Type	Unsigned32
Value	

5.5.2.36 DHCP-RK-Lifetime

WType-ID	42 for DHCP-RK-Lifetime
Description	Lifetime of the DHCP-RK and derived keys.
Value-Type	Unsigned32
Value	Representing the number of seconds the key is valid.

5.5.2.37 DHCPMSG-Server-IP

WType-ID	43 for DHCPMSG-Server-IP
Description	The IPv4 address of the DHCP server contained in the DHCPDISCOVER message.
Value-Type	Address
Value	Octet string containing an IPv4 address of DHCP server (most significant bit first) to which the DHCPDISCOVER/DHCPREQUEST message was sent.

5.5.2.38 Idle-Mode-Transition

WType-ID	44 for Idle-Mode-Transition
Description	A flag indicating whether the mobile node is in idle or not.
Value-Type	Enumerated
Value	Valid values: • Active Mode (0) • Idle Mode (1) All other values reserved.

5.5.2.39 NAP-ID

WType-ID	45 for NAP-ID
Description	Uniquely identifies the Network Access Provider.
Value-Type	OctetString
Value	Three octets representing an operator identifier.

5.5.2.40 BS-ID

WType-ID	46 for BS-ID
Description	Uniquely identifies a NAP and a Base Station within that NAP.
Value-Type	OctetString
Value	6 Octet-String. Representing NAP operator identifier (first 3 Octets) and the Base Station ID (next 3 Octets)

5.5.2.41 Location

WType-ID	47 for Location
Description	Location of the ASN.
Value-Type	UTF8String
Value	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

WType-ID	50 for Flow-Description
Description	Describes a flow classifier.
Value-Type	Classifier
Value	

5.5.2.45 BU-CoA-Ipv6

WType-ID	51 for BU-CoA-IPv6
Description	The CoA from the BU message.
Value-Type	Address
Value	Octet-String representing an IPv6 address as per RFC3588

5.5.2.46 DNS

WType-ID	52 for DNS
Description	The IPv4/IPv6 address of the DNS server to be conveyed to the MS/AMS via DHCP.
Value-Type	Address
Value	An IPv4 or IPv6 address as per RFC3588

5.5.2.47 Hotline-Profile-ID

WType-ID	53 for Hotline-Profile-ID
Description	A unique identifier (relative to the HCSN) of a Hot-Line profile to be applied to this session.
Value-Type	UTF8String
Value	UTF8 String representing a Hot-Line profile formatted as follows: realm + "/" + profile-id-string Where: • Realm is the Fully Qualified Domain Name of the operator that is asserting the Hotline profile; and • Profile-id-string is operator specific label for the hotline profile to be applied at the by the Hot-Lining device.

5.5.2.48 HTTP-Redirection-Rule

WType-ID	54 for HTTP-Redirection-Rule
Description	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.
Value-Type	Grouped

```
HTTP-Redirection-Rule::= < AVP Header: 54>
                    { Redirection-Action }
                    [ Redirect-URL ]                    The redirection URL.
                    * [ IP-Classifier ]                 The matching classifier
                    *[AVP]
```

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-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.

5.5.2.49 IP-Redirection-Rule

WType-ID	55 for IP-Redirection-Rule
Description	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.
Value-Type	Grouped

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-Classifier]	The matching classifier(s).
	*[AVP]	

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.

5.5.2.50 Hotline-Session-Timer

WType-ID	56 for Hotline-Session-Timer
Description	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.
Value-Type	Unsigned32
Value	Representing a time in seconds. A value of zero means infinity.

5.5.2.51 NSP-ID

WType-ID	57 for NSP-ID
Description	Uniquely identifies the Network Service Provider.
Value-Type	OctetString
Value	Octet-String (3 Octets) representing an operator identifier.

5.5.2.52 HA-RK-Key-Requested

Not used.

5.5.2.53 Count-Type

WType-ID	59 for Count-Type
Description	Used to indicate if the record represents compressed or uncompressed counts.
Value-Type	Unsigned32
Value	Unsigned32. When set to (0) indicates uncompressed counts. When set to (1) indicates compressed counts

5.5.2.54 FA-RK-SPI

WType-ID	61 for FA-RK-SPI
Description	The SPI used for the FA-RK.
Value-Type	Unsigned32
Value	Representing a SPI value.

5.5.2.55 vHA-IP-MIP4

WType-ID	64 for vHA-IP-MIP4

Description	The IPv4 address of the vHA for MIP4
Value-Type	Address
Value	An IPv4 address

5.5.2.56 vHA-IP-MIP6

WType-ID	65 for vHA-IP-MIP4
Description	The IPv6 address of the vHA for MIP6
Value-Type	Address
Value	An IPv6 address

5.5.2.57 vDHCPv4-Server

WType-ID	73 for vDHCPv4-Server
Description	The IPv4 or IPv6 address of the visited DHCP Server to use for IPv4 address allocation.
Value-Type	Address
Value	An IPv4 or IPv6 address

5.5.2.58 vDHCPv6-Server

WType-ID	74 for vDHCPv4-Server
Description	The IPv6 address of the visited DHCP Server to use for IPv6 address allocation.
Value-Type	Address
Value	An IPv6 address

5.5.2.59 PMIP-Authenticated-Network-Identity

WType-ID	78 for PMIP-Authenticated-Network-Identity
Description	Identity of the MS/AMS to be used for PMIP operation as the NAI to be included in the PMIP NAI authentication extension.
Value-Type	UTF8String
Value	Contains an identity according to the NAI specification [RFC4282]

5.5.2.60 Visited-Framed-IP-Address

WType-ID	79 for Visited-Framed-IP-Address
Description	The IPv4 home address assigned by the Visited CSN to be used for the MS/AMS.
Value-Type	Address
Value	An IPv4 address

5.5.2.61 Visited-Framed-IPv6-Address

WType-ID	80 for Visited-Framed-IPv6-Address
Description	The IPv4 home address assigned by the Visited CSN to be used for the MS/AMS.

Value-Type	Address
Value	An IPv4 address

5.5.2.62 Visited-Framed-Interface-Id

WType-ID	81 for Visited-Framed-Interface-Id
Description	The IPv6 interface Id assigned by the Visited CSN to be used for the MS/AMS.
Value-Type	OctetString
Value	An IPv4 address

5.5.2.63 Packet-Flow-Descriptor-V2

WType-ID	84 for Packet-Flow-Descriptor-V2
Description	This attribute describes a packet flow. A packet flow may describe a uni-directional flow and bidirectional flow. The packet flow descriptor may be pre-provisioned. A packet flow descriptor references one or two QoS specifications.
Value-Type	Grouped

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]	
[SF-Operation-Policy]	
[Local-Routing-Policy]	
*[AVP]	

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/AMS.
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/AMS.
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/AMS.
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/AMS.
309	UplinkQosID	0-1	This attribute SHALL be present if SerivceProfileId is not present and: Direction is Uplink or Direction is bi-directional and the flow is symmetrical. If ServiceProfileId or either of UplinkQoSID or DownlinkQoSID are missing then the NAS SHALL reject the network entry of the MS/AMS.
310	DownlinkQoSID	0-1	This attribute SHALL be present if SerivceProfileID 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/AMS.
311	IP-Classifier	0-n	This attribute SHALL be present if ServiceProfileID is not present. If either are

TLV ID	TLV Name	Answer	Notes
			missing then the NAS SHALL reject the network entry of the MS/AMS.
470	Local-Routing-Policy	0-1	This attribute MAY only be present when the PDF/PCRF or the AAA and the ASN support the Local Routing Policy.
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.
467	SF-Operation-Policy	0-1	This attribute is to specify the operation policy for the given service flow.

5.5.2.64 VLANTagProcessing-Descriptor

WType-ID	211 for VLANTagProcessing-Descriptor
Description	This attribute describes the rules for the processing of the VLAN tags of an ETH packet flow. The VLANTagProcessing descriptor may be pre-provisioned.
Value-Type	Grouped

VLANTagProcessing-Descriptor::= < AVP Header: 211>

{ VLANTagProcessingRuleID } VLANTagProcessingRuleID = 0 is reserved with special meaning that no VLANTagProcessing is performed for the particular service flow regardless of any preprovisioned rule.

{ C-VLAN-Priority-Setting }

[VLAN-ID-Assignment]

[C-VLAN-ID]

[S-VLAN-ID]

* [C-VID-To-S-VID-Mapping]

[Local-Config-Info] 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]

5.5.2.65 WiMAX®-Release

WTYPE-ID	301 for WiMAX-Release

Description	In a Request specifies the WiMAX release of the sender. In an Answer specifies the release selected by the HAAA for this communication. AAA Proxies SHALL NOT alter the WiMAX-Release values received in an Answer command. If the NAS receives a WiMAX release that it does not support it SHALL treat the result as a rejection. 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.
Value Type	UTF8String
Value	A string indicating a WiMAX release formatted as: major + ”.” + minor. For example, the first release of WiMAX is indicated as “1.0”

1 5.5.2.66 Accounting-Capabilities

WType-ID	302 for Accounting-Capabilities
Description	In a Request describes the accounting capabilities that are supported by the sender (ASN or HA). In an Answer, describes the accounting capabilities that the server selected for the session.
Value-Type	Unsigned32
Value	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. • Bit #0 - IP/ETH-Session-based accounting. Default value for the ASN. • Bit #1 - Flow-based accounting. • Bit #2 - Flow-based accounting for ETH-CS. • Bit #3 – R3-OC based accounting • Bit #4 – R3-OFC based offline accounting 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. All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

2 5.5.2.67 Hotlining-Capabilities

WType-ID	303 for Hotlining-Capabilities
Description	In a Request describes the Hot-Line capacities supported by the ASN or the HA.
Value-Type	Unsigned32
Value	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. • Bit #0 - Profile-based Hot-Lining is supported (using the Hotline-Profile-ID VSA) • Bit #1 - Rule-based Hot-Lining is supported using NAS-Filter-Rule • Bit #2 - Hot-Lining HTTP Redirection is supported. • Bit #3 - Rule-based Hot-Lining is supported using IP-Redirection rule. Bit #1 and Bit #2 SHALL be set as a minimum when the sender is an ASN-GW. All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.68 Idle-Mode-Notification-Capabilities

WType-ID	304 for Idle-Mode-Notification-Capabilities
Description	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.
Value-Type	Unsigned32
Value	In an Access-Request the NAS (ASN) specifies if idle mode notification is supported at the ASN. In Access-Accept the HAAA specifies if idle mode notification is required at the HAAA. • 0x0000 = Idle Mode notification is not supported or is not required. • 0x0001 = Idle Mode notification is supported or is required. • Rest of bits reserved

5.5.2.69 ServiceProfileID

WType-ID	305 ServiceProfileID
Description	This attribute identifies a pre-configure flow descriptor at the NAS.
Value-Type	Unsigned32
Value	Unsigned Integer representing the identity of a Flow Spec that is pre-provisioned (most significant bit first). A value of zero(0) is invalid.

5.5.2.70 Direction

WType-ID	306 for Direction
Description	The direction of the Packet Data Flow.
Value-Type	Enumerated
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = Uplink • 2 = Downlink • 3 = Bi-directional • 4 – FF = Reserved

5.5.2.71 Activation-Trigger

WType-ID	307 for Activation-Trigger
Description	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. If “Dynamic-Reservation” is set to false, the QoS-Descriptor is used to specify a QoS profile for ISFs or pre-provisioned SFs. 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.
Value-Type	Unsigned32
Value	Octet bit-map with the following values: • Bit 0 = Reserved • Bit 1 = Provisioned (SHALL be set in case of ISF) • Bit 2 = Admit (SHALL be set in case of ISF) • Bit 3 = Activate (SHALL be set in case of ISF) • Bit 4 = Dynamic-Reservation(not valid for ISF) All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.72 Transport-Type

WType-ID	308 for Transport-Type
Description	Defines the transport type which might be IP (v4 or v6) as well as Ethernet. This parameter need to be mapped into “CS specification” as defined in IEEE802.16e/m [REF1].
Value-Type	Enumerated
Value	Octet enumeration with the following values: • 0 = Reserved • 1 = IPv4-CS • 2 = IPv6-CS • 3 = Ethernet • 4 – 255 = Reserved

5.5.2.73 UplinkQoSID

WType-ID	309 for UplinkQoSID
Description	The identifier of the QoS descriptor for the uplink direction or for bi-direction if the flow is bi-directional with symmetrical QoS. If the QoSID is not resolvable by the NAS, the NAS SHALL reject the network entry of the MS/AMS. An accounting-stop message with an error reason should be generated.
Value-Type	Unsigned32
Value	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.

5.5.2.74 DownlinkQoSID

WType-ID	310 for DownlinkQoSID

Description	The identifier of the QoS descriptor for the downlink direction. If the QoSID is not resolvable by the NAS, the NAS SHALL reject the network entry of the MS. An accounting-stop message with an error reason should be generated.
Value-Type	Unsigned32
Value	Unsigned Integer (most significant bit first) containing the ID of the QoS descriptor.

5.5.2.75 IP-Classifier

WType-ID	311 for IP-Classifier
Description	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/AMS. An accounting-stop message with an error reason should be generated.
Value-Type	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: • “permit” - Allow packets that match the rule. • “deny” - Drop packets that match the rule. dir: • "in" is from the terminal • "out" is to the terminal. proto: • the ethernet type specified by number. • src and dst MAC address/mask priority-range: • specifies the priority range for the ethernet frame CVLAN-ID: specifies the VLAN-ID range [VID-start, VID-end] for the ethernet frame.

5.5.2.76 QoS-ID

WType-ID	312 for QoS-ID
Description	A unique ID for this QoS specification in this packet. The ID is used in the Service-Flow-Descriptor attribute to reference a specific QoS Spec (see the UplinkQoSID and DownlinkQoSID TLVs)
Value-Type	Unsigned32
Value	An unsigned number less than 256.

5.5.2.77 Global-Service-Class-Name

WType-ID	313 for Global-Service-Class-Name
Description	This parameter represents the Global Service Class Name as defined in IEEE802.16e/m.

Value-Type	OctetString
Value	String of length 6 octet containing the name of the global service class name. Values are defined in IEEE802.16e/m.

5.5.2.78 Service-Class-Name

WType-ID	314 for Service-Class-Name
Description	This parameter represents the Service Class Name as defined in IEEE802.16e/m.
Value-Type	OctetString
Value	String containing the name of the service class name. Values are defined in IEEE802.16e/m.

5.5.2.79 Schedule-Type

WType-ID	315 for Schedule-Type
Description	The parameter specifies the Uplink Granted Scheduling Type as defined in IEEE802.16e/m.
Value-Type	Enumerated
Value	The following values defined: • 0 = Reserved • 1 = Reserved • 2 = Best Effort • 3 = nrtPS • 4 = rtPS • 5 = Extended rtPS • 6 = UGS • 7 – 255 = Reserved Receivers MUST ignore reserved values.

5.5.2.80 Traffic-Priority

WType-ID	316 for Traffic-Priority
Description	The value of this parameter specifies the priority assigned to a service flow. Given two service flows identical in all QoS parameters besides priority, the higher priority service flow should be given lower delay and higher buffering preference. For otherwise non-identical service flows, the priority parameter should not take precedence over any conflicting service flow QoS parameter. The specific algorithm for enforcing this parameter is not mandated here.
Value-Type	Unsigned32
Value	0 to 7 – Higher numbers indicate higher priority. Default 0.

5.5.2.81 Maximum-Sustained-Traffic-Rate

WType-ID	317 for Maximum-Sustained-Traffic-Rate

Description	This parameter defines the peak information rate of the service. The rate is expressed in bits per second and pertains to the SDUs at the input to the system. Explicitly, this parameter does not include MAC overhead such as MAC headers or CRCs. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. If this parameter is omitted or set to zero, then there is no explicitly mandated maximum rate. This field specifies only a bound, not a guarantee that the rate is available. The algorithm for policing to this parameter is left to vendor differentiation and is outside the scope of the standard.
Value-Type	Unsigned32
Value	Unsigned Integer specifying a rate in bits per second.

1 5.5.2.82 Minimum-Reserved-Traffic-Rate

WType-ID	318 for Minimum-Reserved-Traffic-Rate
Description	Represents the Minimum Reserved Traffic Rate as defined in IEEE802.16e/m. 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.
Value-Type	Unsigned32
Value	Unsigned Integer specifying the rate in bytes.

2 5.5.2.83 Maximum-Traffic-Burst

WType-ID	319 for Maximum-Traffic-Burst
Description	Represents the Maximum Traffic Burst as defined in IEEE802.16e. This parameter defines the maximum burst size that SHALL be accommodated for the service. Since the physical speed of ingress/egress ports, the air interface, and the backhaul will in general be greater than the maximum sustained traffic rate parameter for a service, this parameter describes the maximum continuous burst the system should accommodate for the service assuming the service is not currently using any of its available resources.
Value-Type	Unsigned32
Value	Unsigned Integer specifying the burst size in bytes per second as defined by IEEE802.16e/m.

3 5.5.2.84 Tolerated-Jitter

WType-ID	320 for Tolerated-Jitter
Description	Represents the Tolerated Jitter as defined in IEEE802.16e/m.
Value-Type	Unsigned32
Value	Unsigned Integer representing the maximum delay variation (jitter) (in milliseconds).

4 5.5.2.85 Maximum-Latency

WType-ID	321 for Maximum-Latency
Description	Represents the Maximum Latency as defined in IEEE802.16e/m. Time period between the

	reception of a packet by the BS/ABS or MS/AMS 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/ABS or MS/AMS and SHALL be guaranteed by the BS/ABS or MS/AMS. A BS/ABS or MS/AMS does not have to meet this service commitment for service flows that exceed their minimum reserved rate.
Value-Type	Unsigned32
Value	Unsigned Integer specifying a maximum latency in units of milliseconds

1 5.5.2.86 Reduced-Resources-Code

WType-ID	322 for Reduced-Resources-Code
Description	This code indicates that the requesting entity will accept reduced resources if the requested resources are not available.
Value-Type	Unsigned32
Value	A value of 0 is not allowed, value of 1 allowed. Other values are reserved.

2 5.5.2.87 Media-Flow-Type

WType-ID	323 for Media-Flow-Type
Description	Describes the application type, used as a hint in admission decisions, for instance, VoIP, video, PTT, gaming, etc.
Value-Type	Enumerated
Value	An enumeration with the following values: • 0 = Reserved • 1 = Voice over IP • 2 = Robust Browser • 3 = Secure Browser/ VPN • 4 = Streaming video on demand • 5 = Streaming live TV • 6 = Music and Photo Download • 7 = Multi-player gaming • 8 = Location-based services • 9 = Text and Audio Books with Graphics • 10 = Video Conversation • 11 = Message • 12 = Control • 13 = Data • 14 – 255 = Reserved Receivers MUST ignore reserved values.

3 5.5.2.88 Unsolicited-Grant-Interval

WType-ID:	325 for Unsolicited-Grant-Interval
Description:	The value of this parameter specifies the nominal interval between successive data grant opportunities for this service flow. This parameter may be used for UGS and ERT-VR

	service flow when the inter-arrival time of IP packets on the data plane is known in advance (this is typically the case for flows generated by a specific codec).
Value-Type:	Unsigned32
Value:	Value measuring time in milliseconds between 0 and 2^16-1

5.5.2.89 SDU-Size

WType-ID	326 for SDU–Size
Description	Represents the number of bytes in the fixed size SDU. This parameter may be used for a UGS service flow when the length of IP packets on the data plane is fixed and known in advance (this is typically the case for flows generated by a specific codec). If this attribute is absent then the SDU SHALL be variable.
Value-Type	Unsigned32
Value	Value <= 2^16-1. Default = 49

5.5.2.90 Unsolicited-Polling-Interval

WType-ID	327 for Unsolicited-Polling–Interval
Description	The value of this parameter specifies the maximal nominal interval between successive polling grants opportunities for this Service Flow.
Value-Type	Unsigned32
Value	Unsigned integer representing the polling interval (in milliseconds) between 0 and 2^16-1

5.5.2.91 MN-HA-MIP4-MSA

WType-ID	328 for MN-HA-MIP4-MSA
Description	The MN-HA-MIP4-MSA VSA is a grouped AVP that describes the MN-HA security association used for MIP4 service.
Value-Type	Grouped

MN-HA-MIP4-MSA ::= < AVP Header: 328>

{ SA-SPI }	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
[SA-Key]	The MN-HA MIP4 key.
*[AVP]	

AVP	TLV Name	Request	Answer
337	SA-SPI	1	1
338	SA-Key	0	1

5.5.2.92 MN-vHA-MIP4-MSA

WType-ID	329 for MN-vHA-MIP4-MSA
Description	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.
Value-Type	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

WType-ID	330 for FA-RK-MSA
Description	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
Value-Type	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

WType-ID	331 for HA-RK-MSA
Description	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.
Value-Type	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

WType-ID	332 for vHA-RK-MSA
Description	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.
Value-Type	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

WType-ID	333 for DHCP-RK-SA
Description	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.
Value-Type	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

WType-ID	334 for vDHCP-RK-SA
Description	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
Value-Type	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

WType-ID	335 for Redirection-Action
Description	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.
Value-Type	Enumerated
Value	Valid enumeration values are: • PASS(0) • REDIRECT(1) • FLUSH(2) All other values are reserved. Receivers MUST ignore reserved values.

5.5.2.99 Redirect-URL

WType-ID	336 for Redirected-URL
Description	A URL to be used as a redirection response.
Value-Type	UTF8String
Value	A URL as formatted by RFCXXX TBD

5.5.2.100 SA-SPI

WType-ID	337 for SA-SPI
Description	A Security Parameter Index.
Value-Type	Unsigned32
Value	Represents a Security Parameter Index.

5.5.2.101 SA-KEY

WType-ID	338 for SA-KEY
Description	A key.
Value-Type	OctetString

Value	The value of a KEY MSB first.

5.5.2.102 SA-Lifetime

WType-ID	339 for SA-Lifetime
Description	The lifetime in seconds of the security association
Value-Type	Unsigned32
Value	Number of seconds.

5.5.2.103 Redirect-Address

WType-ID	340 for Redirect-Address
Description	The IP address to redirect the traffic to.
Value-Type	Address
Value	The IPv4 address to redirect traffic to

5.5.2.104 Redirect-Port

WType-ID	341 for Redirect-Port
Description	The redirection port to use as the destination port of a redirected packet.
Value-Type	Unsigned32
Value	A port value in the range of 1 to 65356

5.5.2.105 DHCPv6-RK-SA

WType-ID	342 for DHCPv6-RK-SA
Description	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.
Value-Type	Grouped

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]	

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

WType-ID	343 for vDHCPv6-RK-SA
Description	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
Value-Type	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)

WType-ID	344 for Packet-Flow-Descriptor-Capabilities (The usage of this TLV is deprecated in this release. Only Packet-Flow-Descriptor V2 SHALL be supported.)
Description	
Value-Type	
Value	•

5.5.2.108 Authorized-Network-Services

WType-ID	345 for Authorized-Network-Services
Description	This AVP is included in an Answer command to the NAS and indicates related Network Service Capabilities ASN is authorized to support.
Value-Type	Unsigned32
Value	Bit Mask with the following values: • Bit #0 – CMIP4

	• Bit #1 – PMIP4 • Bit #2 – Simple IPv4 • Bit #3 – CMIP6 • Bit #4 – PMIP6 • Bit #5 – Simple IPv6 • Bit #6 – Simple ETH Service • Bit #7 – MIP based ETH Service • Bit #8 – L2 DHCP Relay[a] • The rest of the bits are reserved. The sender SHALL set the reserved bits to zero, and the receiver SHALL ignore the values.

5.5.2.109 ASN-Network-Service-Capabilities

WType-ID	346 for ASN-Network-Service-Capabilities
Description	This AVP is included in a Diameter Request packet to the Diameter server and indicates related Network Service Capabilities ASN is willing to support
Value-Type	Unsigned32
Value	Bit Mask with the following values: • Bit #0 – DHCPv4 Relay • Bit #1 – DHCPv6 Relay • Bit #2 – DHCPv4 Proxy • Bit #3 – DHCPv6 Proxy • Bit #4 – CMIPv4 FA • Bit #5 – PMIPv4 FA and Client • Bit #6 – AR with IPv4 Transport[45] • Bit #7 – AR with IPv6 Transport[46] • Bit #8 – L2FW • Bit #9 – ETH Service FA • Bit #10 – L2 DHCP Relay • Bit #11 - MAG All other bits are reserved. . The sender SHALL set the reserved bits to zero, and the receiver SHALL ignore the values.

[45] AR with IPv4 transport indicates the support of Simple IP service using IPv4 transport

[46] AR with IPv6 transport indicates the support of Simple IP service using IPv6 transport

5.5.2.110 VCSN-Network-Service-Capabilities

WType-ID	347 for VCSN-Network-Service-Capabilities
Description	This AVP is included in a Request packet to the Diameter server and indicates V-CSN related Network Service Capabilities
Value-Type	Unsigned32
Value	Bit Mask with the following values: • Bit #0 – DHCPv4 Server • Bit #1 – DHCPv6 Server • Bit #2 – HAv4 • Bit #3 – HAv6 • Bit #4 – eCB • Bit #5 – ETH HA 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.

5.5.2.111 Visited-Authorized-Network-Services

WType-ID	348 for Visited-Authorized-Network-Services
Description	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.
Value-Type	Unsigned32
Value	Bit Mask with the following values: • Bit #0 – CMIP4 • Bit #1 – PMIP4 • Bit #2 – Simple IPv4 • Bit #3 – CMIP6 • Bit #4 – PMIP6 • Bit #5 – Simple IPv6 • Bit #6 – Simple ETH Service • Bit#7 – MIP based ETH Service • Bit#8 – L2 DHCP Relay[a] All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.112 Paging-Preference

WType-ID	349 for Paging-Preference
Description	This parameter is a single bit indicator of an MS/AMS's preference for the reception of paging advisory messages during idle mode. When set, it indicates that the BS/ABS may present paging advisory messages or other indicative messages to the MS/AMS when data SDUs bound for the MS/AMS are present while the MS/AMS is in idle mode.
Value-Type	Unsigned32
Value	Refer to 802.16e/m section 11.13.30.

5.5.2.113 VLANTagProcessingRuleID

WType-ID	350 for VLANTagProcessingRuleID
Description	The ID of the rules for assigning priority bits and VLAN-IDs in Ethernet frames
Value-Type	Unsigned32
Value	Containing the VLAN Tag Processing Rule ID of the rules for processing the VLAN tags in Ethernet frames

5.5.2.114 Media-Flow-Description-In-SDP-Format

WType-ID	351 for Media-Flow-Description-In-SDP-Format
Description	This is a variable length string having SDP information. The <SDP string> is encoded as specified in IETF RFC 2327
Value-Type	UTF8String
Value	<SDP string> is encoded as specified in IETF RFC 2327.

5.5.2.115 Transmission-Policy

WType-ID	352 for Transmission-Policy
Description	The parameter indicates the transmission policy of a service flow.
Value-Type	Unsigned32
Value	Octet enumeration with the following values defined: • Bit #0 – Service flow SHALL NOT use broadcast bandwidth request opportunities. (Uplink only) • Bit #1 –Service flow SHALL NOT use multicast bandwidth request opportunities. (Uplink only). • Bit #2 – The service flow SHALL NOT piggyback requests with data. (Uplink only) • Bit #3 – The service flow SHALL NOT fragment data. • Bit #4 – The service flow SHALL NOT suppress payload headers (CS parameter). • Bit #5 – The service flow SHALL NOT pack multiple SDUs (or fragments) into single MAC PDUs. • Bit #6 – The service flow SHALL NOT include CRC in the MAC PDU. • Bit #7 – The service flow SHALL NOT compress payload headers using ROHC. All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits. Note: The bit#7 is reserved prior to NWG release 1.5

5.5.2.116 Classifier

WType-ID	353 for Classifier
Description	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/AMS.

Value-Type	Grouped as per [86] with a few modifications as noted below.

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

WType-ID	354 for Classifier-ID
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]. 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.
Value-Type	OctetString as per draft-ietf-dime-qos-attributes-11.txt [86]. In WiMAX the identifier is unique within the scope of the parent container.

5.5.2.118 Priority

WType-ID	355 for Priority
Description	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.
Value-Type	Unsigned32. Value range is between 0 and 255. The higher the value the higher the priority

5.5.2.119 Direction

WType-ID	356 for Direction
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]. The Direction AVP specifies in which direction to apply the Classifier. The values of the enumeration are: "IN","OUT","BOTH". In the "IN" and "BOTH" directions, the From-Spec refers to the address of the Managed Terminal and the To-Spec refers to the unmanaged terminal. In the "OUT" direction, the From-Spec refers to the Unmanaged Terminal whereas the To-Spec refers to the Managed Terminal. If the Direction AVP is omitted, the Classifier matches packets flowing in both directions.
Value-Type	Enumerated as per draft-ietf-dime-qos-attributes-11.txt [86] with the following value • 0 representing IN - The classifier applies to flows from the Managed Terminal • 1 representing OUT - The classifier applies to flows to the Managed Terminal. • 2 representing BOTH - The classifier applies to flows both to and from the Managed Terminal.

5.5.2.120 Action

WType-ID	357 for Action
Description	The values of this field specify the action to either allow packets that match the rule or drop packets that match the rule.
Value-Type	Enumerated with the following values: 0 is Reserved 1 is Permit – Allow packet that match the rule 2 is Deny – Drop packets that match the rule All other values are reserved

5.5.2.121 Protocol

WType-ID	358 for Protocol
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]. Specifies the protocol being matched. The attributes included in the Classifier AVP MUST be consistent with the value of the Protocol AVP. If the Protocol AVP is omitted from the Classifier, then comparison of the protocol of the packet is irrelevant.
Value-Type	Enumerated as per draft-ietf-dime-qos-attributes-11.txt [86]. The values for this AVP are managed by IANA under the Protocol Numbers registry as defined in [36].

5.5.2.122 From-Spec

WType-ID	359 for From-Specification
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]. 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.
Value-Type	Grouped based on the From-Spec AVP of draft-ietf-dime-qos-attributes-11.txt [86]

From-Spec::= < AVP Header: 359>

[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, 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/AMS.
[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/AMS.
[User-Assigned-Address]	This attribute is used only by the network for downlink traffic. It is not sent to the MS/AMS.
[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

WType-ID	360 for To-Specification
Description	As per draft-ietf-dime-qos-attributes-11.txt [86] 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.
Value-Type	Grouped as per draft-ietf-dime-qos-attributes-11.txt [86]

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/AMS.
[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/AMS.
[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/AMS.
[User-Assigned-Address]	This attribute is used only by the network for downlink traffic. It is not sent to the MS/AMS.
[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

5.5.2.124IP-TOS/DSCP-Range-And-Mask

WType-ID	361 for IP-TOS/DSCP-Range-And-Mask
Description	The values of the field specify the matching parameters for the IP type of service/DSCP **[30]** 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.
Value-Type	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.

5.5.2.125ETH-Option

WType-ID	362 for ETH-Option
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]. A grouped TLV with Ethernet specific attributes.
Value-Type	Grouped

ETH-Option::= < AVP Header: 362>

{ ETH-Proto-Type }	
[VLAN-ID-Range]	In WiMAX this attribute may only appear once.
*[ETH-Priority-Range]	
* [AVP]	

5.5.2.126 ETH-Proto-Type

WType-ID	363 for ETH-Proto-Type
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]. Specifies Ethertype and DSAP
Value-Type	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

WType-ID	364 for VLAN-ID-Range
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]. If present, this field specifies the matching values for the VLAN-ID bits. If omitted, the VLAN-ID bits are irrelevant for this entry.
Value-Type	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

WType-ID	365 for ETH-Priority-Range
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]

Value-Type	Grouped

```
ETH-Priority-Range::= < AVP Header: 365>
                      [ ETH-Low-Priority]
                      [ ETH-High-Priority]
                      * [ AVP ]
```

5.5.2.129 ETH-Ether-Type

WType-ID	366 for ETH-Ether-Type
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	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.

5.5.2.130 ETH-SAP

WType-ID	367 for ETH-SAP
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	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.

5.5.2.131 S-VID-Start

WType-ID	368 for S-VID-Start
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Unsigned32 with values between 0 and 4095 inclusive.

5.5.2.132 S-VID-End

WType-ID	369 for S-VID-End
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Unsigned32 with values between 0 and 4095 inclusive.

5.5.2.133 C-VID-Start

WType-ID	370 for C-VID-Start
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Unsigned32 with values between 0 and 4095 inclusive.

5.5.2.134 C-VID-End

WType-ID	371 for C-VID-End
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Unsigned32 with values between 0 and 4095 inclusive.

5.5.2.135 ETH-Low-Priority

WType-ID	372 for ETH-Low-Priority
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Unsigned32 with values between 0 and 7 inclusive.

5.5.2.136 ETH-High-Priority

WType-ID	373 for ETH-High-Priority
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Unsigned32 with value between 0 and 7 inclusive.

5.5.2.137 IP-Address

WType-ID	374 for IP-Address
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Address. IPv4 or IPv6 Address.

5.5.2.138 IP-Address-Range

WType-ID	375 for IP-Address-Range
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Grouped

```
IPAddressRange::= < AVP Header: 375>
                        [IP-Address-Start ]
                        [IP-Address-End ]
                        * [ AVP ]
```

5.5.2.139 IP-Address-Mask

WType-ID	376 for IP-Address-Mask
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Grouped.

```
IP-Address-Mask::= < AVP Header: 376>
                        [ IP-Address ]
                        [ IP-Bit-Mask-Width ]
                        * [ AVP ]
```

5.5.2.140 Port

WType-ID	377 for Port
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Integer32 with a value of 0 to 65535.

5.5.2.141 Port-Range

WType-ID	378 for Port-Range
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Grouped

```
Port-Range::= < AVP Header: 378>
                  [ Port-Start ]
                  [ Port-End ]
                  * [ AVP ]
```

5.5.2.142 Negated

WType-ID	379 for Negated
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Enumerated containing the following values: • TRUE • FALSE All other values reserved

5.5.2.143 User-Assigned-Address

WType-ID	380 for User-Assigned-Address
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Enumerated with values: • TRUE • FALSE All other values reserved.

5.5.2.144 MAC-Address

WType-ID	381 for MAC-Address
Description	As per draft-ietf-dime-qos-attributes-11.txt [86].
Value-Type	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

WType-ID	382 for MAC-Mask
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Grouped

MAC-Mask::= < AVP Header: 382>
[MAC-Address]
[MAC-Address-Mask-Pattern]
* [AVP]

5.5.2.146 IP-Address-Start

WType-ID	383 for IP-Address-Start
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Address. Representing IPv4 or IPv6 address.

5.5.2.147 IP-Address-End

WType-ID	384 for IP-Address-End
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Address. Representing IPv4 or IPv6 address.

5.5.2.148 IP-Bit-Mask-Width

WType-ID	385 for IP-Bit-Mask-Width
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Unsigned32 specifying a number of bits.

5.5.2.149 Port-Start

WType-ID	386 for Port-Start
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Integer32 with value from 0 to 65535 inclusive representing a port number

5.5.2.150 Port-End

WType-ID	387 for Port-End
Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	Integer32 with value from 0 to 65535 inclusive, representing a port number.

5.5.2.151 MAC-Address-Mask-Pattern

WType-ID	388 for MAC-Address-Mask-Pattern

Description	As per draft-ietf-dime-qos-attributes-11.txt [86]
Value-Type	OctetString. The value is 6 octets specifying the bit positions of a MAC address that are taken for matching.

5.5.2.152 C-VLAN-Priority-Setting

WType-ID	389 for C-VLAN-Priority-Setting
Description	Defines the setting of the priority_bits in the C-VLAN tag in the upstream direction.
Value-Type	Unsigned32 representing a bit-field as follows: • 0x00000000 = forward the p_bits without modification • 0x0000001x = drop frames with p_ bits set to a higher value than x • 0x0000002x = set p_bits to x when p_bits set to a higher value than x • 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. Other values reserved

5.5.2.153 VLAN-ID-Assignment

WType-ID	390 for VLAN-ID-Assignment
Description	Defines the processing of the C-VLAN tag and S-VLAN tag
Value-Type	Unsigned32 value representing a bit-field as follows: • 0x00000000 = forward VLAN tags without modification • 0x00000010 = remove S-VID in downstream direction • 0x00000020 = remove C-VID and S-VID, if present, in downstream direction • 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 • 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 • 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 • 0x0000040x = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C->S-VID Mapping table and S-p_bits set to x If no entry exists for a particular C-VID in the C->S-VID Mapping table, the S-VID is set to 0 • 0x00000480 = add S-VLAN tag in upstream to frames with C-VLAN tag with S-VID set according to C->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->S-VID Mapping table, the S-VID is set to 0 Other values reserved. Note: One downstream rule can be combined (ORed) with one upstream rule.

5.5.2.154 C-VLAN-ID

WType-ID	391 for C-VLAN-ID
Description	The value of the field specifies the CVALN ID value for the Ethernet frame.

Value-Type	Unsigned32

5.5.2.155 S-VLAN-ID

WType-ID	392 for MAC-Address-Mask-Pattern
Description	The value of the field specifies the SVALN ID value for the Ethernet frame.
Value-Type	Unsigned32

5.5.2.156 C-VID-To-S-VID-Mapping

WType-ID	393 for C-VID-To-S-VID-Mapping
Description	The value of the field specifies a mapping between a C-VID and a S-VID
Value-Type	Unsigned32. C-VID,S-VID

5.5.2.157 Local-Config-Info

WType-ID	394 for Local-Config-Info
Description	Local configuration information for preprovisioned R3 data path (Simple Ethernet)
Value-Type	OctetString of length n containing arbitrary information The meaning of the information in LocalConfigInfo is subject of static configuration agreements between NAP and NSP.

5.5.2.158 hDHCP-Server-Parameters

WType-ID	86 for hDHCP-Server-Parameters
Description	This attribute contains the Home DHCP server and corresponding security keys.
Value-Type	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

5.5.2.159 vDHCP-Server-Parameters

WType-ID	87 for vDHCP-Server-Parameters
Description	This attribute contains a Visited DHCPv4 server and corresponding security keys.
Value-Type	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

WType-ID	458 for DSCP
Description	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.
Value-Type	Unsigned One Octet representing the DSCP field as defined in RFC2474.

5.5.2.161 BS-Location

WType-ID	88 for BS-Location
Description	In an WDER Command the VSA may be used as an alternative Serving BS/ABS identifier and usually indicates the location information of the BS/ABS which may be described as Lat/Long/Sector/Carrier information of the serving BS/ABS.
Value-Type	UTF8String representing location.

5.5.2.162 Mobility-Access-Classifier

WType-ID	89 for Mobility-Access-Classifier

Description	In a WDEA Command the VSA identifies the classification of the subscriber at the H-AAA as a fixed, nomadic or mobile access subscriber.
Value-Type	Unsigned32 representing an enumeration with the following values: • 1 = Fixed • 2 = Nomadic • 3 = Mobile 4-255= Reserved Receivers MUST ignore reserved values

5.5.2.163 Mobility-Access-Capabilities

WType-ID	395 for Mobility-Access-Capabilities
Description	In a request describes the mobility access capabilities supported by the ASN. Omission of this AVP means fixed/nomadic access is not supported.
Value-Type	Unsigned32. In a Request the NAS (ASN) specifies if fixed/nomadic access is supported at the ASN. • Bit#0 = Fixed/Nomadic access is not supported. Only Mobility. • Bit#1 = Fixed/Nomadic access is supported alongside Mobility. • Bit#2 = Only Fixed/Nomadic access is supported. No Mobility All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.164 ROHC-Support

WType-ID	396 for ROHC-Support
Description	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.
Value-Type	Unsigned32. 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. • Bit #0 = ROHC capability is supported or is required. All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits..

5.5.2.165 R3-OC-Session-Continue

WType-ID	416 for R3-OC-Session-Continue
Description	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. 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”.
Value-Type	Enumerated. The following values are defined:

	FALSE (0) 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. TRUE (1) 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.

5.5.2.166 Old-Session-Id

WType-ID	406 for Old-Session-Id
Description	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. (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.)
Value-Type	UTF8String

5.5.2.167 WiMAX®-Information

WType-ID	409 for WiMAX-Information
Description	The *WiMAX-Information* AVP contains WiMAX access network accounting information for the offline and online charging.
Value-Type	Grouped

```
<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]	
	[Network-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]~~	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.

~~[AF-Charging-Identifier]~~ Only used in case of PCC. See [3] for further details.

[Access-Network-Charging-Identifier-Gx]

[Access-Network-Charging-Address]

[R3-OC-Session-Continue]

[Old-Session-Id]

[Offline-Charging]

5.5.2.168 Uplink-Granted-QoS

WType-ID	30 for Uplink-Granted-QoS
Description	The Uplink-Granted-QoS AVP specifies the Uplink QoS granted to the MS/AMS
Value-Type	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]

5.5.2.169 Downlink-Granted-QoS

WType-ID	63 for Downlink-Granted-QoS

Description	The *Downlink-Granted-QoS* AVP specifies Downlink QoS granted to the MS/AMS.
Value-Type	Grouped

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]

5.5.2.170 Interim-Cause

WType-ID	413 for Interim-Cause
Description	The *Interim-Cause* AVP is used to indicate the reason why the accounting interim message was generated by the accounting client.
Value-Type	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.

5.5.2.171 MS-Authenticated

WType-ID	90 for MS-Authenticated
Description	A flag indicating whether the MS/AMS has successfully performed device authentication during initial network entry or not.

Value-Type	Enumerated. Allowed values: (0) The MS/AMS has not performed device authentication. (1) The MS/AMS has successfully performed device authentication during initial network entry as part of which the MAC address has also been authenticated. All other values reserved

5.5.2.172 Release-Supported

WType-ID	397 for Release-Supported
Description	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.
Value-Type	OctetString. String of supported releases separated by commas ‘,’. The list is ordered from the lowest version to the highest version supported

5.5.2.173 Version-Negotiation-Flag

WType-ID	398 for Version-Negotiation-Flag
Description	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.
Value-Type	Enumerated. Allowed values: (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. (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. (3) Set by the HAAA to indicate that the Diameter WDEA(Multi-round) is for version negotiation only. All other values are reserved.

5.5.2.174 Certified-MS-Feature-List-For-GW

WType-ID	139 for Certified-MS-Feature-List-For-GW
Description	This attribute contains the Certified Feature indication for the MS/AMS to for the GW
Value-Type	Grouped
Value	

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

WType-ID	140 for Certified-MS-Feature-List-For-BS
Description	This attribute contains the Certified Feature indication for the MS/AMS to for the BS/ABS
Value-Type	Grouped
Value	

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/AMS is not certified for any ARQ Capability features

5.5.2.176 Certified-For-MCBCS

WType-ID	459 for Certified-For-MCBCS
Description	Indicates the MCBCS features that the MS/AMS is certified for. The absence of this attribute implies that the MS/AMS is not certified for any MCBCS features.
Value-Type	4 octet OctetString The following one octet Bit-map represent the MCBS features that the MS/AMS is certified for: • Bit-#0 - Certified_for_MCBCS-App • Bit #1 - Certified_for_MCBCS-DSx 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

WType-ID	460 for Certified-For-LBS
Description	Indicates the LBS features that the MS is certified for. The absence of this attribute implies that the MS/AMS is not certified for any LBS features.
Value-Type	4 octet OctetString The following one octet Bit-map represent the LBS features that the MS is certified for: • Bit-#0 - Certified_for_LBS-Control-Plane • Bit #1 - Certified_for_LBS-Hybrid All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.178 Certified-Compression

WType-ID	461 for Certified-Compression
Description	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.
Value-Type	4 octet OctetString, The following one octet Bit-map represent the Compression features that the MS/AMS is certified for: • Bit-#0 - Certified_for_ROHC

	• Bit #1 - Certified_for_PHS All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.179 Certified-Scan-Capability

WType-ID	462 for Certified-Scan-Capability
Description	Indicates the Scan Capability features that the MS/AMS is certified for. The absence of this attribute implies that the MS/AMS is not certified for any Scan Capability features.
Value-Type	4 octet OctetString The following one octet Bit-map represent the Scan Capability features that the MS is certified for: • Bit-#0 – Certified for HO Scanning • Bit-#1 – Certified for Scan Report Type Support • Bit-#2 – Certified for HO/Scan/Report Trigger Metrics All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.180 Certified-Security-Capability

WType-ID	463 for Certified-Security-Capability
Description	Indicates the Security Capability features that the MS/AMS is certified for. The absence of this attribute implies that the MS/AMS is not certified for any Security Capability features.
Value-Type	4 octet OctetString The following one octet Bit-map represent the Security Capability features that the MS/AMS is certified for: • Bit-#0 – Certified for PKM message encoding support • Bit-#1 – Certified for Authorization policy support – Initial Network entry • Bit-#2 – Certified for Authorization policy support – Network re-entry All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.181 Certified-ARQ-Capability

WType-ID	464 for Certified-ARQ-Capability
Description	Indicates the ARQ Capability features that the MS/AMS is certified for. The absence of this attribute implies that the MS/AMS is not certified for any ARQ Capability features.
Value-Type	4 octet OctetString The following one octet Bit-map represent the ARQ Capability features that the MS/AMS is certified for: • Bit-#0 – Certified for Sending and Receiving PDU for ARQ • Bit-#1 – Certified for ARQ feedback message • Bit-#2 – Certified for ARQ Discard message • Bit-#3 – Certified for ARQ Reset message All other bits reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.182 Priority-Indication

WType-ID	465 for Priority-Indication
Description	Priority indication for emergency purposes including ETS.
Value-Type	Unsigned32 with the following values defined: • Bit-#0 – Emergency indication All other bits reserved.

5.5.2.183 Present-Authenticator-Verification-Code

WType-ID	141 for Present-Authenticator-Verification-Code
Description	Present Authenticator Validation Code (MSKHash1)
Value-Type	OctetString (32 octets)

5.5.2.184 OCR-Count

WType-ID	142 for OCR-Count
Description	OCR_COUNT
Value-Type	Counter (2 octets)

5.5.2.185 Packet-Flow-Operation-Policy

WType-ID	466 for Packet-Flow-Operation-Policy
Description	This AVP is present when the serving ASN support the Packet Flow Operation Policy capability, which is used to specify the operation policy to be assigned to a given service flow.
Value-Type	Unsigined32 Integer representing a bit-field with the following definition: Bit-0: Reserved for per SF airlink encrytion on/off capability during the SF establishment. When set to "0", the serving ASN does NOT support per SF airlink encryption on/off capability and when set to "1" the serving ASN supports per SF airlink encyrption on/off capability. All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.186 SF-Operation-Policy

WType-ID	467 for SF-Operation-Policy
Description	This AVP is to specify the operation policy for the given service flow.
Value-Type	Unsigined32 Integer representing a bit-field with the following definition: Bit-0 = "0" - airlink encryption is to be disabled for the given service flow. Bit-0 = "1" - airlink encryption is to be enabled for the given service flow. If the ASN has indicated the support of the SF airlink encryption on/off capability in the Packet-Flow-Operation-Policy, but this parameter is not included, the support of the airlink

	encryption on/off for the given service flow is a local implementation policy of the ASN. All other values are Reserved. The sender shall clear the reserved bits to 0 and the receiver shall ignore the reserved bits.

5.5.2.187 Local-Routing-Indication

WType-ID	244 for Local-Routing-Indication
Description	Indicates whether the service is local routing enabled by ASN GW.
Value-Type	Unsigined32
Value	Bit Mask with the following values: - Bit #0 –Local Routing at ASN-GW All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.188 Local-Routing-Support

WType-ID	269 for Local-Routing-Support
Description	Used to indicate whether Local Routing is supported or not.
Value-Type	Unsigined32
Value	Bitmap. The values are: - Bit #0 – SF-based Local Routing at ASN-GW All other bits are reserved. The sender SHALL set the reserved bits to zero and the receiver SHALL ignore the reserved bits.

5.5.2.189 Local-Routing-Policy

WType-ID	270 for Local-Routing-Policy
Description	Used to specify the Local Routing policy.
Value-Type	Unsigined32
Value	Enumerator. The values are: - 0x00=no ALR - 0x01=Pre-Authorized ALR - 0x02=Dynamic-Authorized ALR All other bits are reserved.

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

WType-ID	263 for Session-Id as specified in [55]

Description	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.
Value-Type	UTF8String

5.5.3.2 Acct-Session-Id

WType-ID	44 for Acct-Session-Id as specified in [55]
Description	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. Note: In WiMAX specific Diameter accounting application, this AVP is used even if the RADIUS/Diameter translation doesn't occur.
Value-Type	OctetString

5.5.3.3 Acct-Multi-Session-Id

WType-ID	50 for Acct-Multi-Session-Id as specified in [55]
Description	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.
Value-Type	Unsigned32

5.5.3.4 Acct-Application-Id

WType-ID	259 for Acct-Application-Id as specified in [55]
Description	The Acct-Application-Id AVP contains the value of TBD defined for WiMAX offline charging application.
Value-Type	Unsigned32

5.5.3.5 NAS-IP-Address

WType-ID	4 for NAS-IP-Address as specified in [63]
Description	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.
Value-Type	OctetString

5.5.3.6 NAS-IPv6-Address

WType-ID	95 for NAS-IPv6-Address as specified in [63]

Description	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.
Value-Type	OctetString

5.5.3.7 Service-Context-Id

WType-ID	461 for Service-Context-Id as specified in [16]
Description	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 based.
Value-Type	UTF8String The format of the Service-Context-Id is: "extensions".NAP.[NSP]."Release"."service-context" "@" "domain" The WiMAX specific values for "service-context" "@" "domain" are: • WiMAX Charging doc#@wimaxforum.org The "tag" indicates the additional feature of the service, e.g. ALR is enabled or not. The tag is encoded as an ASCII string. The tag for ALR is "ALR". Other string values are reserved for future use. The "Release" indicates the WiMAX Release the service specific document is based upon e.g. 1.5 for Release 1.5. As a minimum, Release "service-context" "@" "domain" SHALL be used. If the minimum is used all operator configurable parameters (Oc and Om) are optional. The NAP.[NSP] identifies the operator implementing the service specific document, which is used to determine the specific requirements for the operator configurable parameters. The "extensions" is operator specific information to any extensions in a service specific document.

5.5.3.8 Multiple-Services-Credit-Control

WType-ID	456 for Multiple-Services-Credit-Control as specified in [64]
Description	The Multiple-Services-Credit-Control AVP is specified in IETF RFC 4006 [64] and extended by TS32.299 [100]. 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 [100] needs to be provided. See [3] for more details on this specific case.
Value-Type	Grouped

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

WType-ID	1022 for Access-Network-Charging-Identifier-Gx as specified in [99]
Description	Access-Network-Charging-Identifier-Gx as specified in 3GPP TS29.212 [99]. 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.
Value-Type	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

WType-ID	873 for Service-Information as specified in [100]
Description	The purpose of the *Service-Information* 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.
Value-Type	Grouped

Service-Information :: = < AVP Header: 873 >

~~[Subscription-Id]~~

~~[PS-Information]~~

~~[WLAN-Information]~~

~~[IMS-Information]~~ Only used in case of PCC. See [3] for further details.

~~[MMS-Information]~~

~~[LCS-Information]~~

~~[PoC-Information]~~

~~[MBMS-Information]~~

~~[SMS-Information]~~

[Service-Generic-Information]

[WiMAX-Information]

5.5.3.11 Operator-Name

WType-ID	126 for Operator-Name
Description	This attribute is defined in [97] and contains the country code and the WiMAX assigned company code of the role of the WiMAX operator.
Value-Type	UTF8String

<table>
<tr>
<td><b>Value</b></td>
<td>

The Text field is formatted as follows:

```
 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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-...
```

Where the Namespace ID is as defined by [97] with the value of 0x34 assigned by IANA to WiMAX.

The Operator-Name field is of type Text and is defined by this specification to consist of 3 sub-fields as follows:

The first sub-field consists of a single octet enumeration encoded in ASCII defining the role of the operator as follows:

- “0” (0x30) Reserved
- “1” (0x31) The operator role is a Visited NSP.
- “2” (0x32) The operator role is a Home NSP.
- All other values reserved.

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 for Marine and Satellite operators respectively by the WiMAX Forum.

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”.

</td>
</tr>
</table>

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:

```
 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

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Code      |    Length     |        Enterprise Number1     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |  DataLen1     |               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                          Suboption Data1                      \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Enterprise Number2                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  DataLen2     |             Suboption Data2                   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
\                                                               \
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Code: 9 for the DHCP suboption

Length: >= 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).

```
 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

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type1     |    Length1    |            Value1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
              Value1            |     Type2     |    Length2    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                             Value2                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type3     |    Length3    |            Value3
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
              Value3            | . . . . . . .
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+ . . . . . . .
```

TypeN:

The Type field is one octet. The following values are reserved for the type field and each is explained in a later section.

LengthN:

The one-byte Length field is the length of the data carried in the suboption, in bytes. The length is the length of the data carried in the Value.

ValueN:

The Value field is zero or more octets and contains information specific to the Attribute. The format and length of the Value field are determined by the Type and Length fields.

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	Minimum Data Rate Downstream in kbs	32 bit unsigned integer
0x87	4	Maximum Data Rate Upstream in kbs	32 bit unsigned integer
0x88	4	Minimum Data Rate Downstream 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 5-57 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 5-57 – 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 [58].	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	0-1 [a]	0-1 [a]

		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.		
> 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 2: Handoff between two different interfaces of the mobile node 3: Handoff between mobile access gateways for the same interface 4: Handoff state unknown 5: Handoff state not changed (Re-registration)	1 [b]	1 [b]
> Access Technology Type option	**24**	Set to value 5 for the WiMAX access type	1	1
> Timestamp option	**27**	Set to the current time	1	1
> GRE key option	**TBD**	Set to the downlink GRE key to be used for downlink GRE encapsulated packets	0-1	0-1
> IPv4 Home Address option	**TBD**	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	**TBD**	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	**TBD**	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	**26**	If populated in the PBU it carries the Link-local address of the MAG indicated to the LMA. In the PBA: valid link-layer address for this session to be used by the MAG (generated by LMA or retrieved from the BCE).	**0-1**	0-1

> 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 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 5-58 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 5-58 – 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	**22**	Set to the Home Network Prefix of the MS's connection.	0-1 [a]	0-1 [a]

option				
>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

Type	1 for Notification-Information		
Length in octets	Variable		
Description	The Notification Information is coded as follows:		
Elements (Sub-TLVs)	**TLV Name**	**Description**	**M/O**
	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

Type	2 for Notification-Code
Length in octets	4
Value	32-bit unsigned integer.
Description	Time for MAG-LMA-PMIP6 key remaining valid. This is provided to the MAG by the anchor Authenticator for PMIP6 key context transfer.
Parent TLV(s)	**Notification-Information**

5.8.3 Network Rejection Information

Type	3 for Network Rejection Information		
Length in octets	Variable		
Description	The Network Rejection Information is coded as follows:		
Elements (Sub-TLVs)	**TLV Name**	**Description**	**M/O**
	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.

5.8.4 Rejection Code

Type	4 for Rejection Code
Length in octets	2
Value	The Rejection Code value is defined as follows: **Rejection Class A** – Rejection Codes in the range 0x0000 – 0x00FF • 0x0000 = Rejection Class A – General Error • 0x0001 = Invalid Subscription Information • 0x0002 = Major Network Problem • 0x0003 = Unpaid Bills • 0x0004 = Illegal Mobile Equipment • 0x0005 = Device Type not supported by NSP • 0x0006 = Misbehaving MS Equipment All other Rejection codes in Rejection Class A are undefined. **Rejection Class B** – Rejection Codes in the range 0x0100 – 0x01FF • 0x0100 = Rejection Class B – General Error • 0x0101 = No Roaming Agreement existing with the Home or the Visited Network • 0x0102 = Illegal Mobile Equipment • 0x0103 = Device Type not supported by NSP • 0x0104 = Invalid Subscription/Configuration • 0x0105 = Misbehaving MS Equipment All other Rejection codes in Rejection Class B are undefined. **Rejection Class C** – Rejection Codes in the range 0x0200 – 0x02FF • 0x0200 = Rejection Class C – General Error

- 0x0201 = Invalid Subscription Information
- 0x0202 = Major Network Problem
- 0x0203 = Unpaid Bills
- 0x0204 = Illegal Mobile Equipment
- 0x0205 = Device Type not supported by NSP
- 0x0206 = Misbehaving MS Equipment

All other Rejection codes in Rejection Class C are undefined.

Rejection Class D – Rejection Codes in the range 0x0300 – 0x03FF

- 0x0300 = Rejection Class D – General Error
- 0x0301 = No Roaming Agreement existing with the Home or the Visited Network
- 0x0302 = Illegal Mobile Equipment
- 0x0303 = Device Type not supported by NSP
- 0x0304 = Invalid Subscription/Configuration
- 0x0305 = Misbehaving MS Equipment

All other Rejection codes in Rejection Class D are undefined.

Rejection Class E – Rejection Codes in the range 0x0400 – 0x04FF

- 0x0400 = Rejection Class E – General Error
- 0x0401 = Temporary Network Problem at H-NSP

All other Rejection codes in Rejection Class E are undefined.

Rejection Class F – Rejection Codes in the range 0x0500 – 0x05FF

- 0x0500 = Rejection Class F – General Error
- 0x0501 = No Roaming Agreement existing with the Home or the Visited Network
- 0x0502 = Temporary Network Problem at V-NSP

All other Rejection codes in Rejection Class F are undefined.

Rejection Class G – Rejection Codes in the range 0x0600 – 0x06FF

- 0x0600 = Rejection Class G – General Error
- 0x0601 = Access outside defined Service Area

All other Rejection codes in Rejection Class G are undefined.

Rejection Class H – Rejection Codes in the range 0x0700 – 0x07FF

- 0x0700 = Rejection Class H – General Error
- 0x0701 = No Roaming Agreement existing with the Home or the Visited Network
- 0x0702 = Access outside defined Service Area

All other Rejection codes in Rejection Class H are undefined.

Rejection Class I – Rejection Codes in the range 0x0800 – 0x08FF

- 0x0800 = Rejection Class I – General Error
- 0x0801 = MS equipment not compliant with V-NSP

<table>
<tr><td></td><td>All other Rejection codes in Rejection Class I are undefined.

<b>Rejection Class J</b> – Rejection Codes in the range 0x0900 – 0x09FF<ul><li>0x0900 = Rejection Class J – General Error</li><li>0x0901 = MS equipment not compliant with V-NSP</li></ul>All other Rejection codes in Rejection Class J are undefined.

<b>Rejection Class K</b> – Rejection Codes in the range 0x0A00 – 0x0AFF<ul><li>0x0A00 = Rejection Class K – General Error</li><li>0x0A01 = MS equipment not compliant with H-NSP</li></ul>All other Rejection codes in Rejection Class K are undefined.

All other values are reserved and SHALL be treated as if receiving Rejection Code 0x0000.</td></tr>
<tr><td><b>Description</b></td><td></td></tr>
</table>

5.8.5 Allowed Location Information

<table>
<tr><td><b>Type</b></td><td colspan="3">5 for Allowed Location Information</td></tr>
<tr><td><b>Length in octets</b></td><td colspan="3">Variable</td></tr>
<tr><td rowspan="5"><b>Elements (Sub-TLVs)</b></td><td><b>TLV Name</b></td><td><b>Description</b></td><td><b>M/O</b></td></tr>
<tr><td>BS ID</td><td>Allowed BS/ABS #1</td><td>O</td></tr>
<tr><td>BS ID</td><td>Allowed BS/ABS #2</td><td>O</td></tr>
<tr><td>…</td><td>…</td><td>…</td></tr>
<tr><td>BS ID</td><td>Allowed BS/ABS #n</td><td>O</td></tr>
<tr><td><b>Description</b></td><td colspan="3">The Allowed Location Information may be used as a hint by the MS/AMS</td></tr>
</table>

5.8.6 Received NAI

Type	6 for Received NAI
Length in octets	Variable
Value	The NAI as received from the MS/AMS in the EAP-Identity/Response message during network access authentication and authorization. The NAI is mirrored by the Authenticator to allow the MS/AMS to detect any modification of the NAI and especially the realm portion or routing decoration originally used by the MS/AMS in the (unprotected) EAP-Identity/Response message over-the-air. UTF-8 encoded string without the null character representing the NAI as defined by RFC 4282
Description	

5.8.7 Emergency Services Override

Type	7 for Emergency Services Override

Length in octets	1
Value	Unsigned Octet. Supported values: 0x0000 = Emergency Services Override not supported. 0x0001 = Emergency Services Override supported All other values are reserved, and SHALL be treated as if the Emergency Services Override TLV was not present.
Description	If the MS/AMS 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. If the MS/AMS 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/AMS attempting an emergency network entry may succeed. The Home AAA SHALL NOT send the Emergency Service Override set to “not supported” when the MS is roaming.

5.8.8 RMAC (Rejection Message Authentication Code) Value

Type	8 for RMAC (Rejection Message Authentication Code) Value
Length in octets	32
Value	32 octet RMAC Value SHALL be generated from the EMSK using the following formula: RMAC-Value = HMAC-SHA256(RMAC Key, Network Rejection Information TLV) where: RMAC-1 = HMAC-SHA256(EMSK , usage-data | 0x01) RMAC-2 = HMAC-SHA256(EMSK, RMAC-1 | usage data | 0x02) RMAC-Key = RMAC-1 | RMAC-2 where: usage-data = key label + "\0" + length key label = rmac-key@wimaxforum.org in ASCII length = 0x0200 the length in bits of the RMAC-Key expressed as a 2 byte unsigned integer in network order. 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.

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.

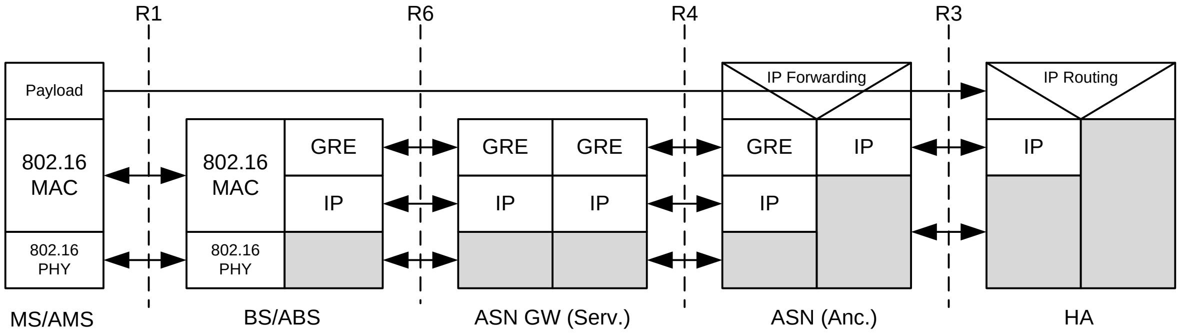


Figure 6-1 – Data Plane with R4 and R6

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 [49] 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/AMS, 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 [29]. 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 [94]. 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 [94]. This IPv6 address must be global unique, and could be either IPv6 global unicast address (RFC3587 [54]), Unique Local IPv6 unicast address (RFC4193 [68]) or IPv4-mapped IPv6 address (RFC4291 [73]). How to assign this IPv6 address is outside the scope of this specification.

6.1.2 GRE Encapsulation

As an option in [49], 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 [95].

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 [49] and extended by [42] 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.

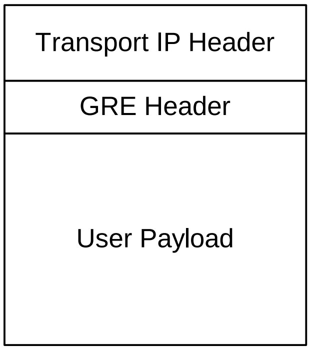


Figure 6-2 – GRE Encapsulation

The GRE protocol according to [37] SHALL be used without the Checksum option. Therefore the Checksum Present bit is set to zero.

[42] 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.

```
   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
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0|0|1|S| Reserved0       |0 0 0|         Protocol Type         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      Key = Data Path ID                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                 Sequence Number (Optional)                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 http://www.iana.org/assignments/ethernet-numbers: • IPv4: 0x0800 • IPv6: 0x86DD • Ethernet: 0x6558 • For the WiMAX Payload Type, 0xFFFF SHALL be used.
Data Path ID	32bit UNSIGNED	Value assigned by the Data Path Function uniquely identifies a particular tunnel for user payload Granularity of tunnels is defined and handled by the DPF.
Sequence Number	32bit UNSIGNED	Optional value for enumerating sequence of user payload packets; may be used for handover enhancements. If the Sequence Number is present in the GRE header, the S-Bit is set to '1'.

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/ABS maps each Data Path ID into a particular MSID and SFID. In this case the mapping table in the BS/ABS is established and maintained by the Data Path Function. The uplink packet classification is taking place in the MS/AMS.

6.3.1 IP-CS

IP datagrams going upstream over R1 are encapsulated in the BS/ABS 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/ABS out of the GRE packet and forwarded over R1 to the MS/AMS. 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/ABS 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/ABS out of the GRE packet and forwarded over R1 to the MS/AMS. 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 MS/AMSs. 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/ABS. The MS/AMSs 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/AMS belonging to the port of the bridge. If multiple CIDs exist in downstream for a particular MS/AMS, classification SHALL be performed in the scope of the CIDs belonging to the MS/AMS. 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 [76]. 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 [84].

Figure 6-4 shows the adoption of the IPoETH-CS link model for the mobile WiMAX network architecture.

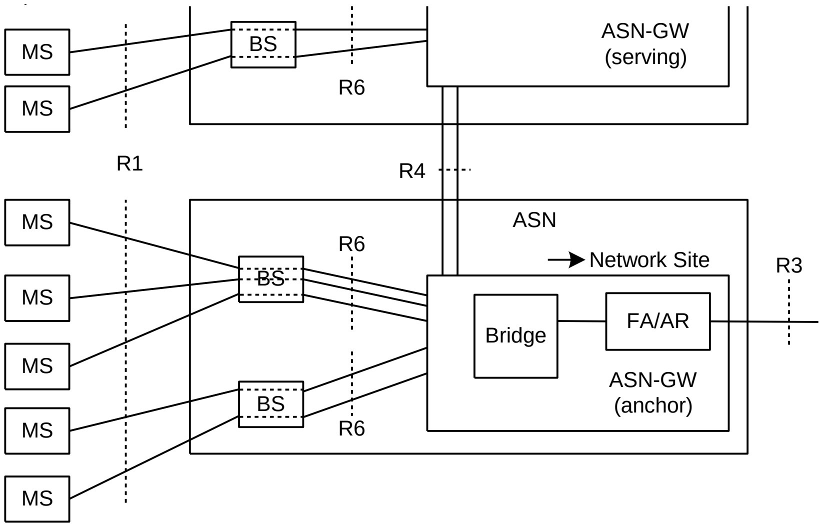


Figure 6-4 – IPoETH-CS Link Model in the WiMAX® Architecture

6.3.3 ETH-CS

Ethernet frames going upstream over R1 are encapsulated in the BS/ABS 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/ABS out of the GRE packet and forwarded over R1 to the MS/AMS. 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/AMS. If multiple CIDs exist in downstream for a particular MS/AMS, classification SHALL be performed in the scope of the CIDs belonging to the MS/AMS. 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 WiMAX Forum® Network Architecture Rel 2

Table 7-1 captures implementation requirements for various features supported in WiMAX Forum® Network Architecture Rel 2. This table lists aspects of the WiMAX Forum® Network Architecture Release 2 specification where two or more solution alternatives are implied and summarizes Mandatory/default and optional choices for implementation of SS/MS/AMS, BS/ABS, 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 WiMAX Forum® Network Architecture Rel 2

Feature	Implementation Requirements (SS/MS/AMS)	Implementation Requirements (BS/ABS)	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 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 unpredictive (uncontrolled) HO	M – Predictive (controlled) and unpredictive (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	7.1 O – CMIPv4 7.2 O – CMIPv6 7.3 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
IP Address Allocation	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
	Fast IP Adress Allocation (Simple-IP)	O	O	O	NA	NA
	DHCP (MIP-based CSN Anchored mobility)	M – DHCPv4 Client O – DHCPv6 Client	NA	M – DHCP Proxy O – DHCP Relay	NA	NA
	Fast IP Adress Allocation (MIP-based CSN Anchored mobility)	O	M	M	NA	NA

Annex A: ASN feature package mapping

Table A-1 – Mapping of ASN feature packages to feature package bit numbers

Feature Package Bit Number	Feature Package Description	Feature Package Identifier
1	ARQ	ARQ_PKG1
2	Basic PHY	BPHY_PKG1
3	Basic Feature Package (MAC_GRP, BWA_GRP, CDM_GRP, NWE_GRP, ISCAN_GRP, IRNG_GRP, SBC_GRP, REG_GRP, PRNG_GRP)	BMAC_PKG1
4	BW Allocation Request	BWA_PKG1
5	BW Allocation Request2	BWA_PKG2
6	Closed Loop Power Control	CLPC_PKG1
7	Coding and Modulation	CODMOD_PKG1
8	Service flow operations	DS_PKG1
9	H-ARQ	HARQ_PKG1
10	MIMO	MIMO_PKG1
11	Idle Mode: MS Initiated Idle	MSIIDM_PKG1
12	Network Topology Acquisition	NTA_PKG1
13	Open Loop Power Control: Passive	OLPC_PKG1
14	Physical CINR	PCINR_PKG1
15	Data Delivery Services for Mobile Network	QPS_PKG1
16	RSSI	RSSI_PKG1
17	Scanning	SCAN_PKG1
18	Synchronization (time/frequency accuracy …)	SYNC_PKG1
19	Channel emission mask (conducted, band specific)	MSK_PKG1
20	Spurious emission mask (conducted, band specific)	SPRE_PKG1

21	Total Radiated Power (TRP) or Near Horizon Total Radiated Power (NHTRP)- Cat 1	TRP_PKG1
22	Total Isotropic Sensitivity (TIS) or Near Horizon Total Isotropic Sensitivity (NHTIS)- Cat 1	TIS_PKG1
23	Intermediate Channel Sensitivity (ICS)- Cat 1	ICS_PKG1
24	Total Radiated Power (TRP) or Near Horizon Total Radiated Power (NHTRP)- Cat 2	TRP_PKG2
25	Total Isotropic Sensitivity (TIS) or Near Horizon Total Isotropic Sensitivity (NHTIS)- Cat 2	TIS_PKG2
26	Intermediate Channel Sensitivity (ICS)- Cat 2	ICS_PKG2
27	Internet Protocol (IPv4)	IPv4_PKG1
28	PHS	PHS-PKG1
29	MS Initiated Controlled Handover	MSIHO_PKG1
30	Security	SEC_PKG1
31	MS Initiated Network Exit	MS-Initiated-NetExit-PKG1
32	Network Initiated Network Exit	Net-Initiated-NetExit-PKG1
33	Unpredictive or Uncontrolled Handover	Uncontrolled-Handover-PKG1
34	PHS	PHS-PKG1
35	MS Initiated Controlled Handover	MS-Initiated-HO-PKG1