

Attachment 4-2-10

WiMAX Forum[®] Network Architecture

Architecture, detailed Protocols and Procedures

Policy and Charging Control

WMF-T33-109-R015v01

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



WiMAX Forum[®] Network Architecture

Architecture, detailed Protocols and Procedures
Policy and Charging Control

WMF-T33-109-R015v01

WiMAX Forum[®] Approved
(2009-11-21)

WiMAX Forum Proprietary

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

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

Copyright 2007-2009 WiMAX Forum. All rights reserved.

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

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

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

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

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

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

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

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

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

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

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

TABLE OF CONTENTS

1.	REVISION HISTORY.....	7
2.	DOCUMENT SCOPE.....	7
3.	ABBREVIATIONS AND DEFINITIONS	7
3.1	Abbreviations	7
3.2	Terms & Definitions.....	9
3.2.1	<i>WiMAX IP-CAN Bearer</i>	<i>9</i>
3.2.2	<i>WiMAX IP-CAN Bearer Binding.....</i>	<i>9</i>
3.2.3	<i>WiMAX IP-CAN Session</i>	<i>9</i>
3.2.4	<i>WiMAX IP-CAN Session Binding.....</i>	<i>9</i>
3.2.5	<i>WiMAX Flow Mapping to PCC.....</i>	<i>9</i>
4.	REFERENCES.....	10
5.	REQUIREMENTS AND PRINCIPLES	11
6.	NETWORK REFERENCE MODEL.....	12
6.1	Reference architecture	12
6.1.1	<i>Non-roaming architecture.....</i>	<i>12</i>
6.1.2	<i>Roaming architecture.....</i>	<i>12</i>
6.1.3	<i>Diameter Based Online Charging Architecture</i>	<i>13</i>
6.2	Functional elements and reference points.....	14
6.2.1	<i>Functional Entities</i>	<i>14</i>
6.2.1.1	PCRF	14
6.2.1.2	Policy Distribution Function (PDF).....	14
6.2.1.3	C-PCEF.....	14
6.2.1.4	A-PCEF.....	15
6.2.1.5	Accounting Client	15
6.2.1.6	Serving-SFA	15
6.2.1.7	Accounting Agent	15
6.2.1.8	OCS/OFCS	15
6.2.1.9	Application Function (AF).....	15
6.2.1.10	AAA.....	15
6.2.1.11	Subscription Profile Repository (SPR)	16
6.2.2	<i>Reference Points.....</i>	<i>16</i>
6.2.2.1	Gx (Ty) Reference Point.....	16
6.2.2.2	PCC-R3 Reference Point	16
6.2.2.3	R4 Reference Point	16
6.2.2.4	Rx/Tx Reference Point.....	16
6.2.2.5	Gy/Gz Reference Point	16
6.2.2.6	Sp Reference Point.....	16
6.2.2.7	PCC-roaming Reference Point.....	16
7.	FUNCTIONAL DESCRIPTION.....	17
7.1	Overall description	17
7.2	General	17
7.2.1	<i>Binding mechanism</i>	<i>17</i>
7.2.2	<i>Reporting.....</i>	<i>17</i>
7.2.3	<i>Credit management</i>	<i>17</i>
7.2.4	<i>Event triggers</i>	<i>17</i>

PCC

1	7.3	Policy and charging control rule	18
2	7.4	QoS Mappings	18
3	8.	PROCEDURES AND FLOWS	19
4	8.1	Service Flow Management	19
5	8.1.1	Initial Service Flow and Pre-Provisioned Service Flow creation	19
6	8.2	Session establishment	20
7	8.3	Session termination	22
8	8.3.1	MS/SS/BS initiated Session Termination	23
9	8.3.2	A-PCEF initiated Session Termination	25
10	8.3.3	PCRF initiated Session Termination	26
11	8.4	Session modification	27
12	8.4.1	PCRF Initiated Session Modification	27
13	8.4.2	SPR Triggered Session modification	29
14	8.4.3	A-PCEF Initiated Session Modification	30
15	8.5	Handling mobility	31
16	8.5.1	A-PCEF relocation	31
17	8.6	Procedures and Flows for Online Charging	33
18	8.6.1	Session Establishment	33
19	8.6.1.1	Initial and Pre-Provisioned Service Flow Creation	33
20	8.6.2	Session Termination	35
21	8.6.2.1	MS/SS/BS Initiated	35
22	8.6.2.2	ASN Initiated	36
23	8.6.2.3	PCRF Initiated	37
24	8.6.3	Session Modification	38
25	8.6.3.1	PCRF Initiated	38
26	8.6.3.2	ASN Initiated	39
27	8.6.4	Handling Mobility	40
28	9.	MESSAGE AND PARAMETER DEFINITIONS	41
29	9.1	PCC Framework Negotiation	41
30	9.2	PCC-R3-OC Support Negotiation	41
31	9.2.1	Online Charging Capability Exchange with PCC Framework	41
32	9.3	Radius protocol extensions for R3 authentication	42
33	9.3.1	ASN PCC Capabilities TLV in WiMAX Capabilities VSA	42
34	9.3.2	PCC-R3-OC Specific Value Definition	42
35	9.4	Definition of PCC-R3-P Reference Point	42
36	9.4.1	PCC Procedures over PCC-R3-P reference point	43
37	9.4.1.1	Bearer Binding	43
38	9.4.2	Diameter based PCC-R3-P Protocol	43
39	9.4.2.1	Initialization, maintenance and termination of connection and session	43
40	9.4.2.2	PCC-R3-P specific AVPs	43
41	9.4.2.3	PCC-R3-P Re-Used AVPs	46
42	9.4.2.4	PCC-R3 Messages	50
43	9.4.3	Radius based PCC-R3-P Protocol	52
44	9.4.3.1	PCC-R3-P specific Radius VSAs	53
45	9.4.3.2	PCC-R3-P re-used attributes and VSAs	66
46	9.4.3.3	Messages for Radius based PCC-R3-P	66
47	9.5	Diameter Based Offline Charging	71
48	9.5.1	PCC-R3-OFC Reference Point	72
49	9.5.2	PCC-R3-OFC' Reference Point	72
50	9.5.3	Triggering Events for Accounting-Request Messages	72
51	9.5.4	Overview of Diameter AVPs used for PCC-R3-OFC and PCC-R3-OFC' Reference points	73
52	9.5.5	Accounting Messages over PCC-R3-OFC Reference Point	78
53	9.5.5.1	Accounting-Request Message	78

PCC

1	9.5.5.2	Accounting-Answer Message	79
2	9.5.6	AVP Occurrence Table.....	79
3	9.5.7	Accounting Messages over PCC-R3-OFC' Reference Point.....	82
4	9.5.7.1	Accounting-Request Message.....	82
5	9.5.7.2	Accounting-Answer Message	83
6	9.5.8	AVP Occurrence Table.....	83
7	9.6	Diameter based Online Charging.....	85
8	9.6.1	PCC-R3-OC Interface Definition	86
9	9.6.1.1	Initialization, maintenance and termination of connection and session	86
10	9.6.1.2	PCC-R3-OC specific AVPs	86
11	9.6.1.3	PCC-R3-OC Re-Used AVPs of external organizations	87
12	9.6.1.4	PCC-R3-OC Messages	90
13	9.6.2	Mobility handling	100
14	9.7	PCC-R3-OC and PCC-R3-OFC AVP definitions.....	100
15	9.7.1	Common AVPs used for WiMAX offline and online charging.....	100
16	9.7.1.1	Service-Information	101
17	9.7.1.2	WiMAX-Information AVP	101
18	9.7.1.3	AF-Charging-Identifier	102
19	9.7.2	Offline Charging specific AVPs.....	102
20	9.7.2.1	Access-Network-Charging-Identifier-Value	102
21	9.7.2.2	Access-Network-Charging-Address	103
22	9.7.2.3	SDFID.....	103
23	9.7.2.4	PDFID.....	103
24	9.7.2.5	Uplink-Flow-Description.....	103
25	9.7.2.6	Downlink-Flow-Description	103
26	9.7.2.7	Uplink-Granted-QoS.....	103
27	9.7.2.8	Downlink-Granted-QoS.....	104
28	9.7.2.9	Direction	104
29	9.7.2.10	Charging-Information	104
30	9.7.3	Online Charging specific AVPs.....	104
31	9.7.3.1	Multiple-Services-Credit-Control AVP	104
32	9.7.3.2	Hotlining-Capabilities.....	105
33	9.7.3.3	Hotlining- Indicator	105
34	10.	HANDLING ERROR CASES.....	106
35	10.1	Types of Error Cases	106
36	10.1.1	Disconnection with peer entity – Type I.....	106
37	10.1.2	Delayed or no response (timeout) – Type II.....	106
38	10.1.3	Response with failure result – Type III.....	106
39	10.2	General Principle	107
40	10.2.1	IP-CAN session establishment.....	107
41	10.2.2	IP-CAN session termination.....	107
42	10.2.3	IP-CAN session modification	107
43	10.2.3.1	The error handling of A-PCEF	107
44	10.3	States Synchronization	108
45	10.3.1	Reporting PCC Rules Status.....	108
46	10.3.2	States Synchronization Flow	108
47	10.1	Failure Code	109
48	ANNEX A	INTERWORKING WITH 3GPP PCC.....	110
49	ANNEX B	INTERWORKING WITH 3GPP2 PCC.....	110
50	ANNEX C	ROAMING ARCHITECTURE WITH HA IN THE VISITED NETWORK	110

PCC

1	ANNEX D QOS MAPPING (INFORMATIVE)	110
2	ANNEX E ASN PROCEDURES FOR INTERWORKING WITH PCC FRAMEWORK	
3	(INFORMATIVE)	111
4	E. 1 Session establishment.....	111
5	E. 2 Session termination.....	113
6	E.2.1 MS/BS initiated.....	113
7	E.2.2 MS initiated IP address release.....	115
8	E.2.3 A-PCEF initiated.....	116
9	E.2.4 PCRF initiated.....	118
10	E. 3 Session modification.....	119
11	E.3.1 PCRF initiated.....	119
12	E.3.2 A-PCEF initiated.....	121
13	E.3.3 BS-initiated bearer termination.....	122
14	E. 4 Handling mobility.....	124
15	E.4.1 A-PCEF relocation.....	124
16	ANNEX F EXAMPLES FOR ERROR HANDLING	127
17	F. 1 Type I Failure	127
18	F. 2 Type II Failure	127
19	F. 3 Type III Failure.....	128
20	F. 4 The Error Handling During the IP-CAN Session Establishment.....	129
21	ANNEX G AN EXAMPLE OF STATES SYNCHRONIZATION	130
22		
23		
24	LIST OF FIGURES	
25	FIGURE 1: MAPPING OF WIMAX FLOWS TO PCC FLOWS.....	10
26	FIGURE 2: WIMAX PCC ARCHITECTURE – NON-ROAMING SCENARIO.....	12
27	FIGURE 3: WIMAX POLICY CONTROL ARCHITECTURE – ROAMING SCENARIO WITH HA IN THE	
28	HOME NETWORK.....	13
29	FIGURE 4: DIAMETER BASED ONLINE CHARGING ARCHITECTURE	13
30	FIGURE 5: PRE-PROVISIONED SERVICE FLOW CREATION.....	19
31	FIGURE 6: SESSION ESTABLISHMENT	21
32	FIGURE 7: MS/BS INITIATED IP-CAN SESSION TERMINATION	23
33	FIGURE 8: A-PCEF INITIATED IP-CAN SESSION TERMINATION	25
34	FIGURE 9: PCRF INITIATED IP-CAN SESSION TERMINATION	26
35	FIGURE 10: PCRF INITIATED IP-CAN SESSION MODIFICATION.....	28
36	FIGURE 11: SPR TRIGGERED SESSION MODIFICATION.....	29
37	FIGURE 12: A-PCEF INITIATED IP-CAN SESSION MODIFICATION.....	30
38	FIGURE 13: A-PCEF RELOCATION.....	32
39	FIGURE 14: INITIAL AND PRE-PROVISIONED SERVICE FLOW CREATION.....	34
40	FIGURE 15: MS INITIATED IP-CAN SESSION TERMINATION	35
41	FIGURE 16: ASN INITIATED IP-CAN SESSION TERMINATION	36
42	FIGURE 17: PCRF INITIATED IP-CAN SESSION TERMINATION	37
43	FIGURE 18: PCRF INITIATED IP-CAN SESSION MODIFICATION.....	38
44	FIGURE 19: ASN INITIATED IP-CAN SESSION MODIFICATION	39
45	FIGURE 20: END TO END OFFLINE CHARGING SCENARIO	72
46	FIGURE 21: STATES SYNCHRONIZATION FLOW	108
47	FIGURE 22: WIMAX PCC ROAMING ARCHITECTURE WITH HA IN THE VISITED NETWORK	110
48	FIGURE 23: ASN PROCEDURES FOR IP-CAN SESSION ESTABLISHMENT	112

PCC

1	FIGURE 24: ASN PROCEDURES FOR MS/ BS-INITIATED SESSION RELEASE (NETWORK EXIT)	114
2	FIGURE 25: ASN PROCEDURES FOR IP HOST INITIATED SESSION RELEASE	115
3	FIGURE 26: ASN PROCEDURES FOR A-PCEF INITIATED SESSION RELEASE	117
4	FIGURE 27: ASN PROCEDURES FOR PCRF INITIATED IP-CAN SESSION RELEASE	118
5	FIGURE 28: ASN PROCEDURES FOR PCRF INITIATED IP-CAN SESSION MODIFICATION	120
6	FIGURE 29: ASN PROCEDURES FOR MS INITIATED IP-CAN SESSION MODIFICATION	121
7	FIGURE 30: ASN PROCEDURES FOR BS INITIATED BEARER TERMINATION	123
8	FIGURE 31: ASN PROCEDURES FOR A-PCEF RELOCATION	125
9	FIGURE 32: EXAMPLE OF TYPE I FAILURE	127
10	FIGURE 33: EXAMPLE OF TYPE II FAILURE	128
11	FIGURE 34 : EXAMPLE OF TYPE III FAILURE (SESSION ESTABLISHMENT FAILURE)	128
12	FIGURE 35 : EXAMPLE OF TYPE III FAILURE (PCC RULE FAILURE)	128
13	FIGURE 36 : EXAMPLE FOR THE ERROR HANDLING OF IP CAN SESSION ESTABLISHMENT WITH	
14	NETWORK EXIT	129
15	FIGURE 37 : EXAMPLE OF STATE SYNCHRONIZATION	130

17 LIST OF TABLES

18	TABLE 1: PCC-R3-P SPECIFIC AVPS	44
19	TABLE 2: PCC-R3-P RE-USED DIAMETER AVPS	47
20	TABLE 3: PCC-R3-P RE-USED RADIUS ATTRIBUTES AND VSAS	66
21	TABLE 4: RADIUS MESSAGES FOR PCC-R3-P	68
22	TABLE 5: AAA MESSAGES AND THEIR TRIGGERING EVENTS	72
23	TABLE 6: IETF REUSED AVPS	74
24	TABLE 7: 3GPP REUSED AVPS	75
25	TABLE 8: WIMAX SPECIFIC AVPS	76
26	TABLE 9: AVP OCCURRENCE TABLE	80
27	TABLE 10: AVP OCCURRENCE TABLE	84
28	TABLE 11: PCC-R3-OC SPECIFIC AVPS	87
29	TABLE 12 : PCC-R3-OC RE-USED DIAMETER AVPS	88
30	TABLE 13: CREDIT-CONTROL-REQUEST MESSAGE CONTENT	92
31	TABLE 14: CREDIT-CONTROL-ANSWER MESSAGE CONTENT	97
32	TABLE 15: RECOMMENDED QOS PARAMETERS TRANSLATION	110

33

34

1. Revision History

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

2. Document Scope

The scope of this document is to specify the Policy and Charging Control (PCC) framework for WiMAX. The PCC framework allows applications like IMS applications to dynamically request QoS and charging attributes for a specified service data flow from the access network where the framework verifies the authorization for the requested QoS.

The PCC framework for WiMAX is based on the Release 7 PCC solution of the Third Generation Partnership Project (3GPP). An online and offline charging is also provided in this document.

3. Abbreviations and Definitions

3.1 Abbreviations

3GPP	3 rd Generation Partnership Project
3GPP2	3 rd Generation Partnership Project 2
AAA	Authentication, Authorization, and Accounting
ABNF	Augmented Backus-Naur Form
AF	Application Function
A-PCEF	PCEF in the ASN
ASN	Access Service Network
ASP	Access Service Provider
AVP	Attribute Value Pair
BE	Best Effort
CCA	Credit Control Answer
CCR	Credit Control Request
CDR	Charging Data Record
COA	Change of Authorization
C-PCEF	PCEF in the CSN
CSN	Connectivity Service Network
DEA	Diameter-EAP-Answer
DM	Disconnect Message
DP	Data Path

PCC

DPF	Data Path Function
EAP	Extensible Authentication Protocol
eRT-VR	Extended Real-Time Variable Rate
HAAA	Home Network AAA
hCSN	Home Network CSN
H-PCRF	PCRF in the Home Network
HoA	Home Address
IMS	Internet Multimedia Subsystem
IP-CAN	IP Connectivity Access Network
ISF	Initial Service Flow
MS	Mobile Subscriber
NAP	Network Access Provider
NAS	Network Attached Storage
NASREQ	Code name for Diameter Network Access Server Application draft-ietf-aaa-diameter-nasreq-17.txt Application.
NRT-VR	Non Real-Time Variable Rate
OCS	Online Charging System
OFCS	Offline Charging System
PCC	Policy and Charging Control
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PD	Packet Data
PDF	Policy Distribution Function
PDFID	Policy Data Flow Identity
PF	Policy Function
PP	Pre-Paid
PPC	Prepaid Client
PPS	Prepaid Accounting Server
PPSF	Pre-Provisioned Service Flow
RAA	Re-Auth-Answer
RAR	Re-Auth-Request
SDFID	Service Data Flow Identifier
SF	Service Flow
SFA	Service Flow Authorization
SFM	Service Flow Management

PCC

TLV	Tag/Length/Value
TS	Technical Specification
UGS	Unsolicited Grant Service
vCSN	Visited Network CSN
VSA	Vendor Specific Attribute
WCAR	WiMAX Change of Authorization Request

- 1
- 2 **3.2 Terms & Definitions**
- 3 **3.2.1 WiMAX IP-CAN Bearer**
- 4 A WiMAX IP-CAN bearer is one or a pair of service flows (one uplink and one downlink service flow) with a
- 5 defined QoS parameter set as specified in [1].
- 6 **3.2.2 WiMAX IP-CAN Bearer Binding**
- 7 WiMAX IP-CAN bearer binding is the association between PCC rules and WiMAX Service Flows. .
- 8 **3.2.3 WiMAX IP-CAN Session**
- 9 A WiMAX IP-CAN session is the association between an MS and an IP network. The association is identified by a
- 10 user IP address (HoA in case of MIP) together with the Subscription ID. A WiMAX IP-CAN session is established
- 11 after an IP address is assigned to the MS through DHCP or MIP, and terminated when the IP address assigned to the
- 12 MS is released.
- 13 **3.2.4 WiMAX IP-CAN Session Binding**
- 14 WiMAX IP-CAN session binding is the association of the AF (Application Function) session and applicable PCC
- 15 rules to a WiMAX IP-CAN session as defined in [2]. It is performed by the PCRF at AF session establishment,
- 16 modification, or termination.
- 17 **3.2.5 WiMAX Flow Mapping to PCC**
- 18 Figure 1 depicts the mapping of WiMAX flows to PCC flows.

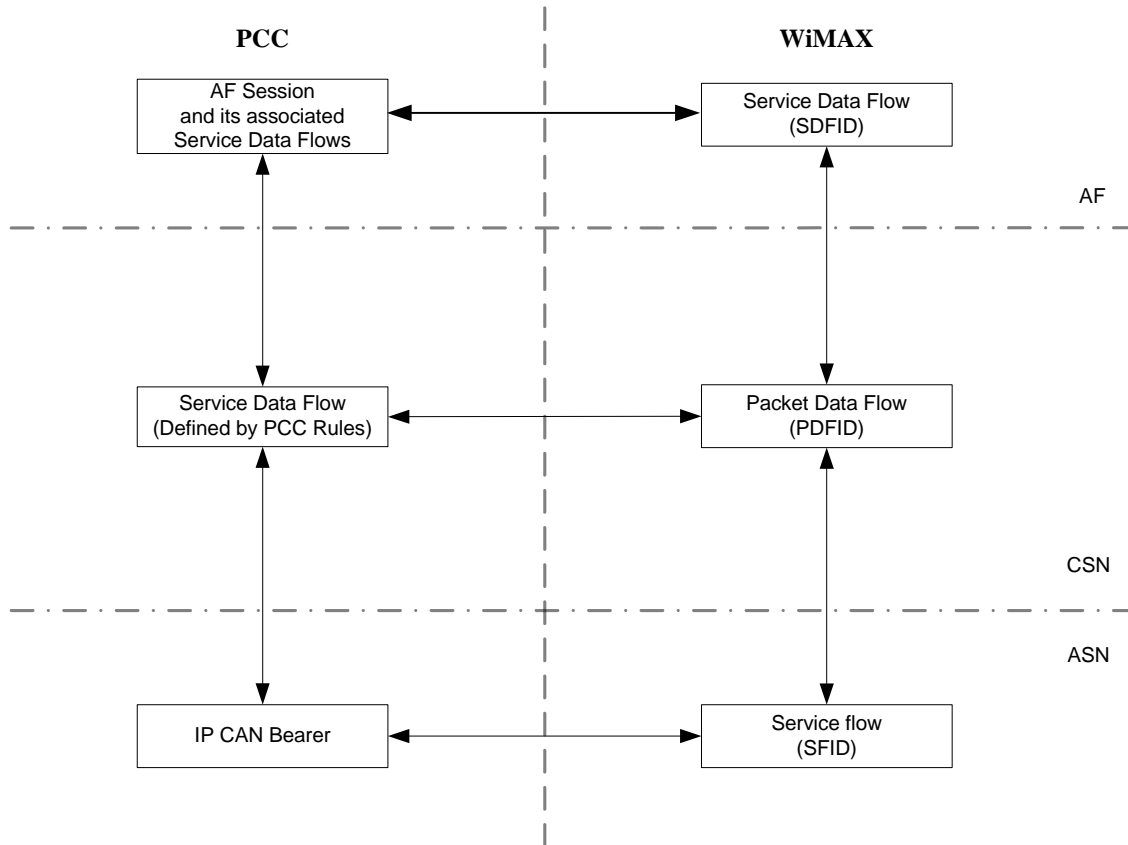


Figure 1: Mapping of WiMAX flows to PCC flows.

An AF session [2] and its associated service data flows correspond to a WiMAX service data flow which is identified by the SDFID [11]. A WiMAX service data flow provides a data service to a user. It consists of one or more packet data flows, each flow corresponding to a media component of such a service.

A 3GPP service data flow is defined by PCC rules. It corresponds to a WiMAX packet data flow which is identified by the PDFID. A WiMAX packet data flow is bound to a WiMAX service flow (or two if the packet data flow is bi-directional).

In WiMAX, pre-provisioned service flows (PPSFs), including the initial service flows (ISFs), are defined as WiMAX packet data flows. When under PCC control, PCC rules may be applied to PPSFs.

4. References

- [1] IEEE Std 802.16-2004: Air Interface for Fixed Broadband Wireless Access Systems
- [2] 3GPP TS 23.203 V7.6.0: Policy Control and Charging Architecture
- [3] 3GPP TS 29.212 "Policy and Charging Control over Gx reference point", Release 7
- [4] 3GPP TS 29.213 "Policy and Charging Control signalling flows and QoS parameter mapping", Release 7
- [5] 3GPP TS 29.214 "Policy and Charging Control over Rx reference point", Release 7
- [6] 3GPP TS 29.229 "Cx and Dx interfaces based on the Diameter protocol", Release 7
- [7] 3GPP TS 32.240 "Charging architecture and principles", Release 7

PCC

- [8] 3GPP TS 32.295 “Charging management; Charging Data Record (CDR) transfer”, Release 7
- [9] 3GPP TS 32.299 “Charging management; Diameter charging applications”, Release 7
- [10] WiMAX Forum, T32-001-R015v01 “Architecture Tenets, Reference Model and Reference Points”, Release 1.5
- [11] WiMAX Forum, T33-001-R015v01 “Detailed Protocols and Procedures, Base Specification”, Release 1.5
- [12] 3GPP2 X.S0013-012 “Service Based Bearer Control –Stage - 2”
- [13] 3GPP2 X.S0013-013 “Service Based Bearer Control –Tx Interface Stage - 3”
- [14] 3GPP2 X.S0013-014 “Service Based Bearer Control –Ty Interface Stage - 3”
- [15] IETF RFC 4005 “Diameter Network Access Server Application”
- [16] IETF RFC 4006 "Diameter Credit-Control Application"
- [17] IETF RFC 4566 "SDP: Session Description Protocol"
- [18] IETF RFC 3588 "Diameter Base Protocol"
- [19] 3GPP TS 23.401 “General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access”, Release 8
- [20] Recommendation and Requirements for Network based on WiMAX Forum Certificate Products, SPWG Release 1.5, 12/04/2007

5. Requirements and Principles

PCC related requirements are specified in [20].

6. Network Reference Model

6.1 Reference architecture

This section describes the architectural model for the WiMAX PCC solution that conforms to the requirements and principles of Section 5.

6.1.1 Non-roaming architecture

Figure 2 illustrates the architectural view of WiMAX PCC which includes both standalone WiMAX networks as well as 3GPP/2 Interworking for the non-roaming scenario.

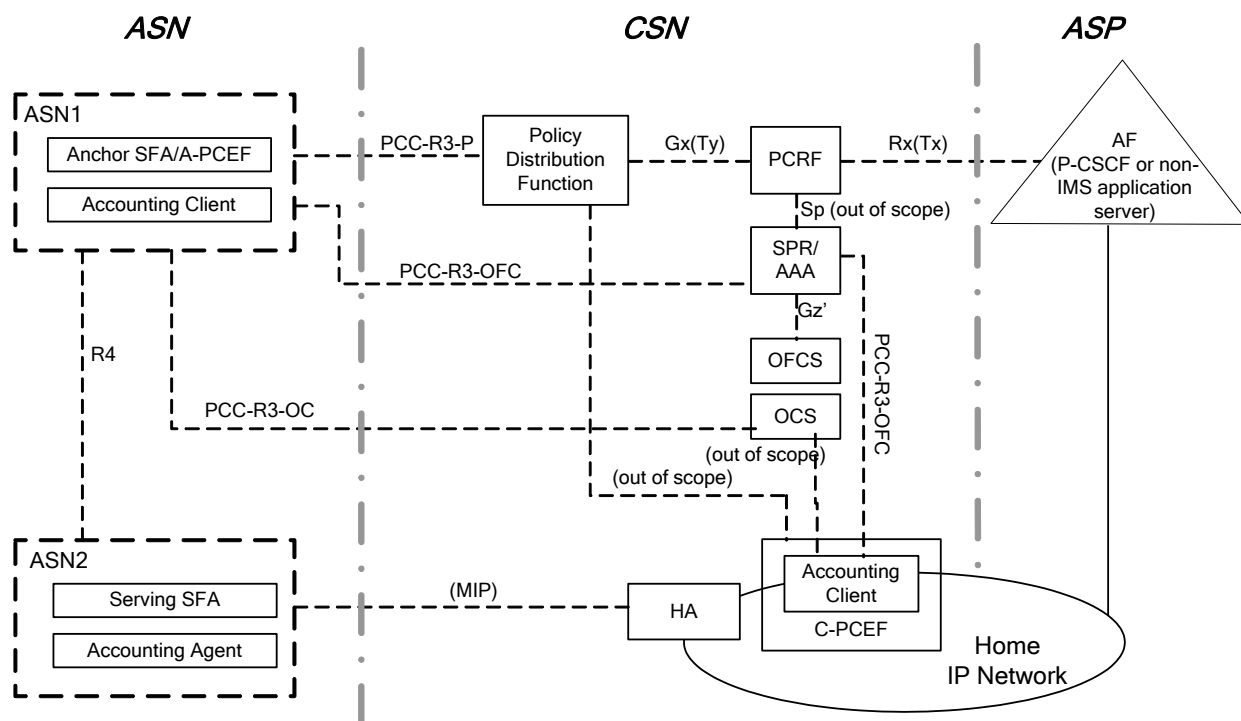


Figure 2: WiMAX PCC architecture – non-roaming scenario.

Note: Details of the C-PCEF as well as the reference points between the C-PCEF and other entities are outside the scope of the current specification.

6.1.2 Roaming architecture

Figure 3 illustrates the roaming architecture for WiMAX Policy Control framework with HA in the home network. Roaming architecture with HA in the visited network is presented in Informative Annex C.

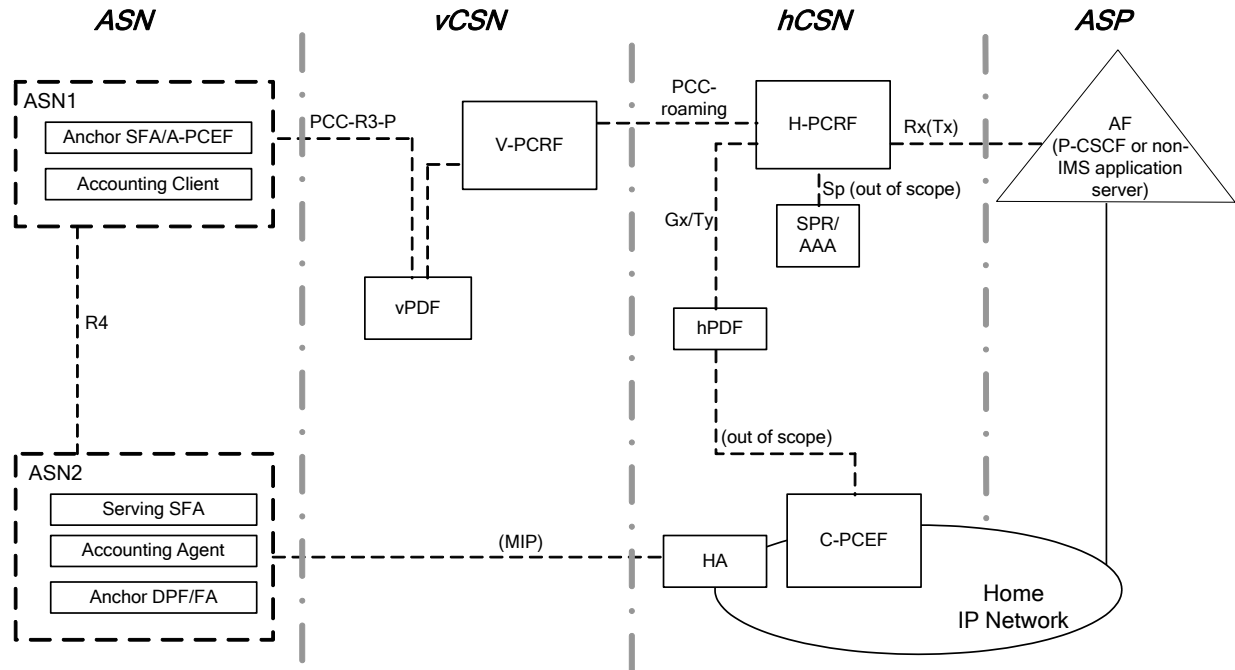


Figure 3: WiMAX Policy Control architecture – roaming scenario with HA in the home network.

6.1.3 Diameter Based Online Charging Architecture

Figure 4 illustrates the diameter based online charging architecture. It involves three entities: the Prepaid Client (PPC), the Prepaid Agent (PPA), and the Prepaid Server (PPS), described in Section 4.4.3.3 of [11]. The architecture has the following characteristics:

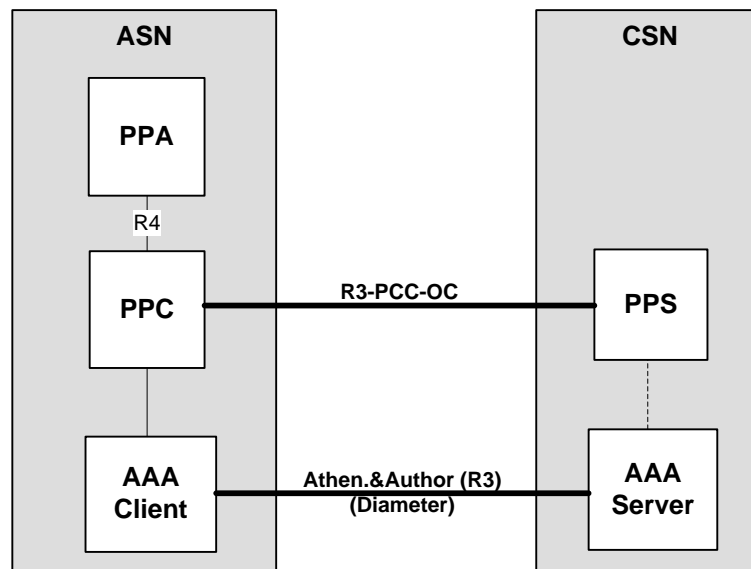


Figure 4: Diameter based online charging architecture

1. This architecture applies to both non-PCC and PCC supported scenarios.
2. When a Service Flow is created/deleted, PPC will request/return credit from/to PPS for the SF. Since in WiMAX PCC the SF is equivalent to the bearer, this procedure is the same for PCC and non-PCC supported scenarios as both cases are based on Service Flow.

PCC

3. There might be an interface between the PCC and the AAA client to allow the AAA to perform a quota balance check during the network entry. This interface between the PCC and the AAA Client is out of the scope of this specification.
4. In roaming scenarios, Authentication and Authorization as well as Diameter Credit Control Application signaling is routed from the ASN through Diameter proxy agents in the visited CSN to the Diameter servers in the home CSN per [18] with no WiMAX specific extensions.

6.2 Functional elements and reference points

6.2.1 Functional Entities

6.2.1.1 PCRF

The PCRF is equivalent to the 3GPP and 3GPP2 defined PCRF [2][12]. In the WiMAX PCC framework, the PF [10] is replaced by the PCRF which is connected to the PDF via the Gx/Ty reference point. The PCRF encompasses policy control decision and flow based charging control functionalities. The PCRF performs session binding (i.e., the association of the AF session information and applicable PCC rules to an IP-CAN session) and PCC rule authorization.

6.2.1.2 Policy Distribution Function (PDF)

The Policy Distribution Function (PDF) is a logical function that enables interworking with 3GPP/2 PCC framework and has the following characteristics:

- The PDF is connected to the PCRF through Gx (Ty) reference point and from the PCRF's point of view the PDF is the termination point of Gx (Ty) reference point.
- The PDF hides the distributed nature and mobility of WiMAX enforcement points from the PCRF. The PDF is connected to the Anchor SFA in the ASN via PCC-R3-P interface and supports SFA relocation by decoupling PCC-R3-P sessions from Gx/Ty.
- The PDF is the distribution point for the PCC rules between the ASN and the CSN; it proxies Gx (Ty) messages over PCC-R3-P between the PCRF and the A-PCEF. However, the interface between PDF and C-PCEF is out of the scope of the current specification.

Note: The physical location of the PDF within the CSN is an implementation choice, i.e., it is an implementation option whether the PDF functionality resides in a standalone network entity, with the PCRF, or with any other network entity. The standalone PDF is well suited for interworking a WiMAX access network with an existing 3GPP/2 PCRF. The integrated PDF/PCRF is well suited for supporting a WiMAX access network with the enhanced QoS capabilities of the WiMAX access technology.

6.2.1.3 C-PCEF

The C-PCEF is the policy and charging enforcement point in the CSN and has the following characteristics:

- The C-PCEF is an optional enforcement point for the IP-level policies and/or charging and its functions are a subset of the PCEF functions as defined in [2][12].
- The C-PCEF is on the bearer path and has full access to the user plane.
- The C-PCEF communicates to the PDF.
- The C-PCEF communicates to the OCS for online charging.
- The C-PCEF communicates to the AAA for offline charging.

Note: The physical location of C-PCEF within the CSN is an implementation choice.

Note: Some functions in the C-PCEF may require awareness of IP session establishment and teardown. The definition of control plane interfaces between the C-PCEF and CSN entities other than PDF, if needed, is out of scope of this document.

PCC

6.2.1.4 A-PCEF

The A-PCEF is responsible for the enforcement of PCC rules and/or charging in the ASN.

The A-PCEF in the Anchor SFA is the termination point for PCC-R3-P reference point. The Anchor SFA is collocated with the Accounting Client and communicates over R4/R6 with the other ASN enforcement points like SFM¹, Serving SFA and Accounting Agent, and is responsible for:

- Serving as the PCEF in the ASN (A-PCEF) by receiving PCC rules from PCC-R3 reference point.
- Relaying charging information to the collocated Accounting Client, and sending WiMAX bearer information (WiMAX Service Flow structure, which includes QoS requirements and packet classification rules) to Serving SFA / Anchor DPF.
- Mapping between IP-level QoS provided in PCC rules and WiMAX Access QoS
- Performs the bearer binding.

6.2.1.5 Accounting Client

The Accounting Client is defined in [10] and is responsible for:

- Receiving the charging information in the PCC rule and forwarding it as WiMAX per-SF accounting information to Accounting Agent
- Collecting the accounting information from Accounting Agent and relaying it to the OCS via the PCC-R3-OC interface for online charging and to the AAA via PCC-R3-OFC interface for offline charging, respectively.

6.2.1.6 Serving-SFA

The Serving-SFA is defined in [9] and is responsible for:

- The enforcement of QoS and service flow level policies over the ASN reference points
- Relaying accounting information between Accounting Agent and the Accounting Client in the anchor SFA.

6.2.1.7 Accounting Agent

The Accounting Agent is defined in [10] and is the enforcement point of charging in the ASN. Additionally, it is responsible for:

- Enforcing charging policy of PCC rule and generating offline accounting information
- Reporting accounting information to accounting client

6.2.1.8 OCS/OFCS

The OCS defined in [2] provides the credit information to the A-PCEF/C-PCEF, and/or acknowledges the credit report via the PCC-R3-OC reference point if online charging is applicable.

The OFCS defined in [2] is used for collecting offline charging record via the PCC-R3-OFC reference point.

Note: The OFCS might be collocated with the AAA or might be a separate entity.

6.2.1.9 Application Function (AF)

The WiMAX IP-CAN imposes no additional requirements to the AF functionalities defined in [2] and [12].

6.2.1.10 AAA

The AAA enables interworking between the WiMAX flow based charging and the 3GPP/2 PCC charging, and has the following characteristics:

- The AAA proxies offline accounting messages from the accounting client to the OFCS.

¹ Note: The ASN entities such as the Serving-SFA, SFM as well as the interfaces R4 and R6 are specified in [9].

PCC

- The AAA is connected to the OFCS through PCC-R3-OFC' reference point and from the OFCS's point of view the AAA is the termination point of PCC-R3-OFC' reference point.

6.2.1.11 Subscription Profile Repository (SPR)

SPR is out of scope of this specification.

6.2.2 Reference Points**6.2.2.1 Gx (Ty) Reference Point**

Gx (Ty) is defined between the PCRF and the PDF.

Gx (Ty) is defined in [3] ([14]).

Gx/Ty reference point is Diameter based.

6.2.2.2 PCC-R3 Reference Point

PCC-R3 reference point includes PCC-R3-P, PCC-R3-OC, and PCC-R3-OFC interfaces.

PCC-R3-P protocol is defined between PDF and A-PCEF/Anchor SFA and runs over R3. This interface carries extensions of the Gx (Ty) interface and enables proxing of the PCC policies to the ASN.

PCC-R3-OC protocol is defined between OCS and A-PCEF and runs over R3. This interface is based on extensions of the 3GPP Gy interface, with extensions as needed.

PCC-R3-OFC protocol is defined between the Anchor SFA and AAA and runs over R3.

6.2.2.3 R4 Reference Point

R4 reference point and necessary extensions for PCC are specified in [10] and [11].

6.2.2.4 Rx/Tx Reference Point

WiMAX PCC imposes no new requirements to the Rx/Tx reference point defined in [3][13].

6.2.2.5 Gy/Gz Reference Point

Gy and Gz interfaces are online and offline charging interfaces, respectively, defined in 3GPP.

6.2.2.5.1 PCC-R3-OFC' Interface

The interface between OFCS and AAA is an extension to 3GPP defined Gz [8][9], extended with optional WiMAX specific attributes.

Note that [8] and [9] define GTP-based (Ga interface) and Diameter-based (Rf interface) offline charging protocols, respectively. Details of the PCC-R3-OFC' interface can be found in Section 9.5.7.

6.2.2.6 Sp Reference Point

Sp reference point is out of scope of this specification.

6.2.2.7 PCC-roaming Reference Point

PCC-roaming reference point is defined between the two PCRFs in the home and visited networks.

PCC-roaming reference point consists Gx/Ty used when the PDF is not included as part of the H-PCRF and V-PCRF.

Note: WiMAX imposes no new requirements to the Gx'/Ty reference point defined in [2][12].

7. Functional Description

7.1 Overall description

WiMAX PCC framework specified in this document is based on 3GPP PCC Rel 7. This section only describes the WiMAX specific functions of the WiMAX PCC architecture and one should refer to 3GPP PCC Rel 7 specifications for detailed functional description of PCC entities not presented here.

7.2 General

7.2.1 Binding mechanism

As explained in [2], the bearer binding mechanism is the procedure that associates a service data flow to the IP-CAN bearer. Thus, the binding mechanism shall associate the AF session information with the IP-CAN bearer that is intended to carry the service data flow.

The binding mechanism in PCC framework includes three different steps: session binding, PCC rule authorization and bearer binding. WiMAX binding specifies:

1- Session binding, i.e., the association of the AF session information and related PCC rules to an IP-CAN session. The PCRF shall perform the session binding, which shall take into account the information about the packet data network the user is accessing, in addition to the user IP address and the user identity, if available.

2- PCC rule authorization, i.e., the selection of a QoS class identifier for the PCC rule, shall be performed by the PCRF. Each PCC rule includes a QoS class identifier that can be supported by WiMAX.

3- Bearer binding, i.e., the association of the PCC rule to an IP-CAN bearer (i.e. a WiMAX SF) within that IP-CAN session. For WiMAX the Anchor SFA/A-PCEF performs the bearer binding as defined in [2].

7.2.2 Reporting

As described in [2], reporting refers to the differentiated IP-CAN bearer usage information (measured at the PCEF) being reported to the online or offline charging functions. The reporting requirements specified for PCEF in [2] shall apply to A-PCEF.

7.2.3 Credit management

Credit is managed based on the Diameter Credit Control Application (DCCA) [15] and PCC Release 7 extensions [8] with the credit control client residing in the A-PCEF and the credit control server in the OCS. DCCA allows real-time credit management by the client requesting and obtaining a reservation of credit called a quota. Unused portions of a quota are returned to the server after service delivery completes. Quotas can be obtained for entire user sessions or for particular flows (services) within a session. WiMAX systems are able to leverage DCCA to charge for multiple such services within a single session at different rates while drawing from a common pool of credit. WiMAX extensions involve only the necessary AVPs to describe access specific parameters. Additionally for WiMAX, this specification supports mobility where the credit control client may be relocated while credit control continues for the user sessions and all services contained within.

7.2.4 Event triggers

In addition to the event triggers specified in [2] the following event triggers shall apply for WiMAX:

On the PCC-R3-P Interface:

-A-PCEF relocation event trigger: this trigger is an indication to the PDF that no new session creation has occurred, instead, following an A-PCEF relocation, the session is continued.

- Anchor-Data-Path-Change event trigger: this trigger is an indication to the PDF that Serving SFA relocation has occurred.

PCC

7.3 Policy and charging control rule

PCC-R3-P, PCC-R3-OFC and PCC-R3-OC follow policy and charging control rule handling as defined in [2]. In case of IP-CAN session establishment, pre-provisioned QoS profile may be included at the IP-CAN session request to allow further policy check by the PCRF.

7.4 QoS Mappings

The QoS-Information in the PCC rule represents the authorized QoS for the IP flow as defined in [3]. The QoS class identifier (QCI) in the QoS-information is scalar used as a reference to node specific parameters that control packet forwarding treatment in the QoS-Information and accommodates the need for differentiating QoS in all types of IP-CANs.

The A-PCEF SHALL allow operator specific mapping between QoS-Information AVP and WiMAX bearer parameters.

Annex D presents an example of a QoS mapping.

8. Procedures and Flows

This section provides the WiMAX PCC signaling flows based on the signaling flows provided in [2] and [4].

In the offline charging procedure, accounting interim message(s) may be sent from the accounting client to the AAA between the accounting start and the accounting stop messages.

Details of intra-ASN internal interactions that generate or receive IP-CAN triggers are not part of this chapter. ASN internal details are specified in the WiMAX base specification [11]. The linking of IP-CAN triggers and ASN flows are shown in Annex E.

8.1 Service Flow Management

8.1.1 Initial Service Flow and Pre-Provisioned Service Flow creation

Figure 5 applies to Initial Service flow and pre-provisioned service flow creation. The QoS profiles of the pre-provisioned service flows are provided by the Home AAA Server while rules for supporting dynamic service flows are provided by the PDF/PCRF if PCC is supported.

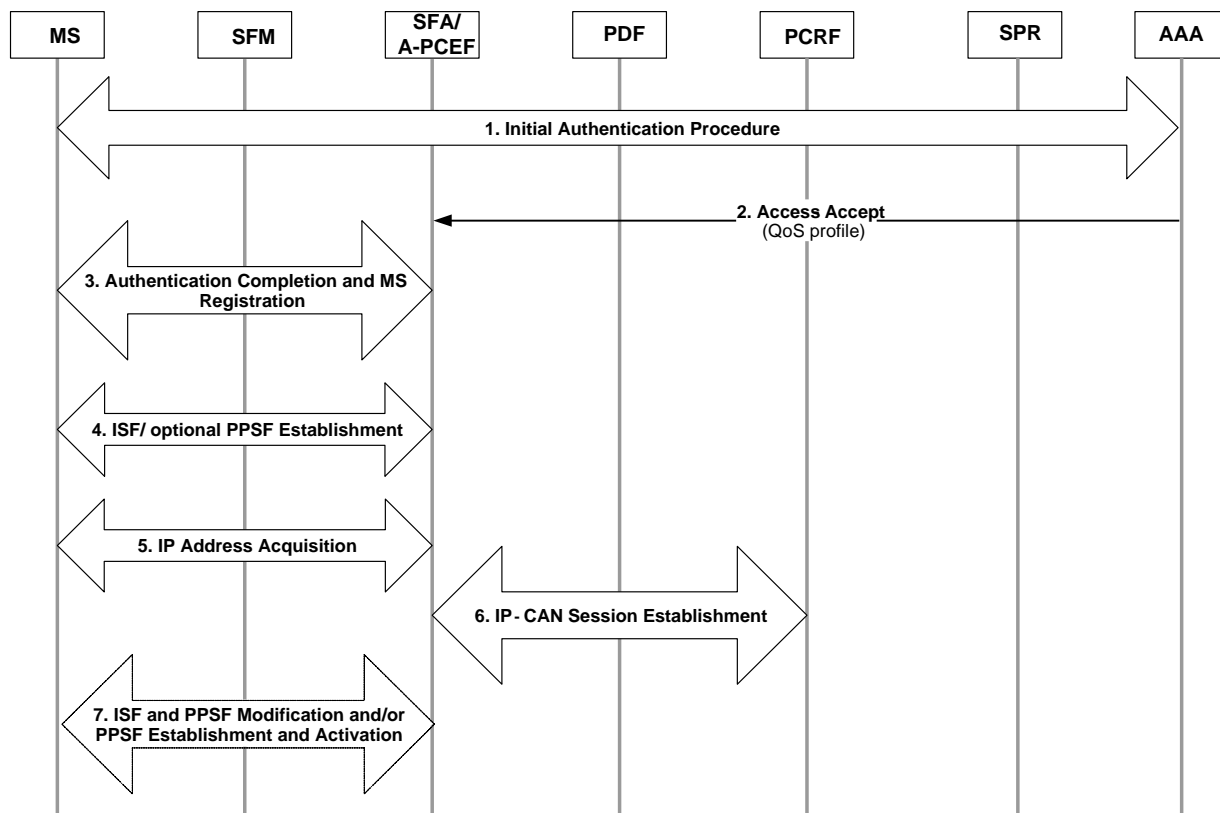


Figure 5: Pre-provisioned service flow creation

1. Authenticator detects the completion of EAP-based Authentication by receiving Initial Access-Accept message.
2. The AAA server provides the user's QoS profile of the Pre-Provisioned Service Flows together with charging information to the Anchor SFA.
3. Authenticator proceeds with EAP authentication completion and obtaining the required security keys. After the completion of PKMv2 procedures, MS performs network a registration procedure.

PCC

4. Anchor SFA detecting MS registration completion, initiates ISF establishment and if applicable, the Pre-provisioned Service Flows (PPSF) establishment. Anchor SFA MAY delay the establishment of other PPSFs until IP address acquisition or until step (7).
5. MS acquires an IP address (e.g. DHCP, MIP).
6. The A-PCEF proceeds with IP-CAN session establishment with the PDF/PCRF. The Anchor-SFA/A-PCEF SHALL send an IP-CAN Session Establishment request to the PDF. The Anchor SFA/A-PCEF SHALL include the QoS profile obtained from AAA server during step 2 to authorize the QoS policies. The IP-CAN session is established as defined by PCC IP-CAN session establishment procedure in Section 8.2. The PCRF MAY acquire the user QoS subscription profile from the SPR. As a result of the QoS policies authorization, the PDF/PCRF MAY modify the ISF and/or PPSF and notify the Anchor SFA/A-PCEF in the response.
7. If the PCC rules from the PDF/ PCRF are different from the QoS profile received from AAA at the end of the authentication procedure, the Anchor SFA/A-PCEF SHALL modify the QoS of the ISF, and if applicable, the PPSFs. The Anchor SFA SHALL relay the charging policy to the collocated accounting client. If only ISF was established in step (4), the Anchor SFA SHALL initiate the establishment of the PPSFs according to the PCC rules received from the PDF/ PCRF. The Serving SFA/ Anchor DP, collocated with Anchor SFA at the time of initial network entry, installs the received IP and QoS policies and also enforces the authorized QoS for the PPSFs.

8.2 Session establishment

- An IP-CAN session is initiated in WiMAX after the IP-address allocation to the user is completed.
- Figure 6 is applicable if a new IP-CAN session is being established.
- When the session establishment procedure occurs in the Non-Roaming case, the V-PCRF is not involved.
- In the case of roaming the V-PCRF is employed to forward messages from the H-PCRF in the home network, by way of the V-PCRF in the visited network to the ASN.
- This procedure applies to the scenario where user accesses home services.

PCC

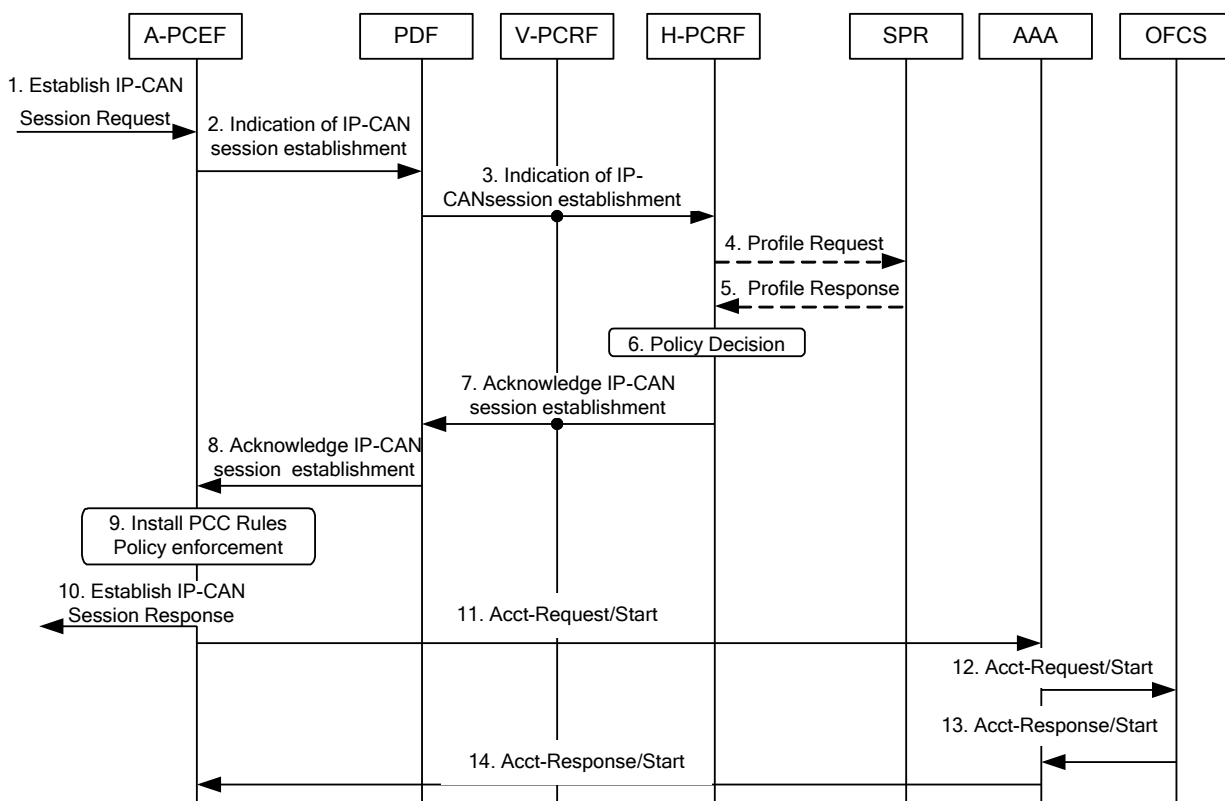


Figure 6: session establishment

1. The A-PCEF receives an Establish IP-CAN Session Request. The A-PCEF accepts the request and assigns an IP address for the user.
2. The A-PCEF determines that the PCC authorization is required, requests the authorization of allowed service(s) and PCC Rules information. The A-PCEF includes the following information: IP-CAN type (WiMAX), and if available, the default charging method and the IP-CAN bearer establishment modes supported. The A-PCEF also includes MS identity information (MS NAI) and the MS IPv4 address and/or MS IPv6 address prefix and the A-PCEF IP address/identity.
3. The PDF processes the information received from A-PCEF and determines that H-PCRF should be contacted and forwards the relevant information received from the A-PCEF to the H-PCRF (by way of the V-PCRF in the roaming case).
4. If the H-PCRF does not have the subscriber's subscription related information, it sends a request to the SPR in order to receive the information related to the IP-CAN session. The H-PCRF provides the subscriber ID to the SPR. The H-PCRF may request notifications from the SPR on changes in the subscription information.
5. The H-PCRF stores the subscription related information containing the information about the allowed services and PCC rules information.
6. The H-PCRF makes the authorization and policy decision.
7. The H-PCRF sends the decision(s), including the bearer-control mode, to the PDF (by way of the V-PCRF in the roaming case). The H-PCRF may provide the default charging mode.

PCC

8. The PDF acknowledges the establishment of the IP-CAN session to the A-PCEF. PCEF-relocation AVP is included in the list of PCC-R3-P event triggers. If applicable, PDF updates the list of event triggers to include other PCC-R3-P specific triggers.
9. The A-PCEF enforces the decision(s). The A-PCEF will relay the QoS policy and service flow level policies to serving SFA/ Anchor DPF and SFM via R4/ R6 reference points using service flow and data path control procedures (as presented in [13]). The Serving SFA (Anchor DPF) will enforce the received IP policies and SFM (BS) will enforce service flow level QoS policies over the air. Note that enforcement of QoS policies in SFM is subject to Admission Control and the request may be rejected by SFM. The A-PCEF will also relay the charging policy to a collocated accounting client after receiving the authorized PCC rules. The accounting client will relay the charging policy to accounting agent for charging enforcements.
10. If at least one PCC rule was successfully activated, the A-PCEF acknowledges the Establish IP-CAN Session Request.
11. The A-PCEF sends accounting start message(s) to the AAA, based on the flow based accounting. The accounting start message is generated per each packet data flow.
12. For offline charging, the AAA sends accounting start message(s) to the OFCS.
13. The OFCS acknowledges the Accounting Start Request.
14. The AAA acknowledges the Accounting Start Request.

8.3 Session termination

A WiMAX IP-CAN session is terminated when the MS IP address is released.

Note that sleep mode and idle mode impose no change to an IP-CAN session.

When the session termination procedure occurs in the Non-Roaming case, the V-PCRF is not involved.

In the case of roaming the V-PCRF is employed to forward messages from the H-PCRF in the home network, by way of the V-PCRF in the visited network to the ASN.

This procedure applies to the scenario where user accesses home services.

8.3.1 MS/SS/BS initiated Session Termination

Figure 7 is applicable if a WiMAX IP-CAN session is being released by the MS or the BS.

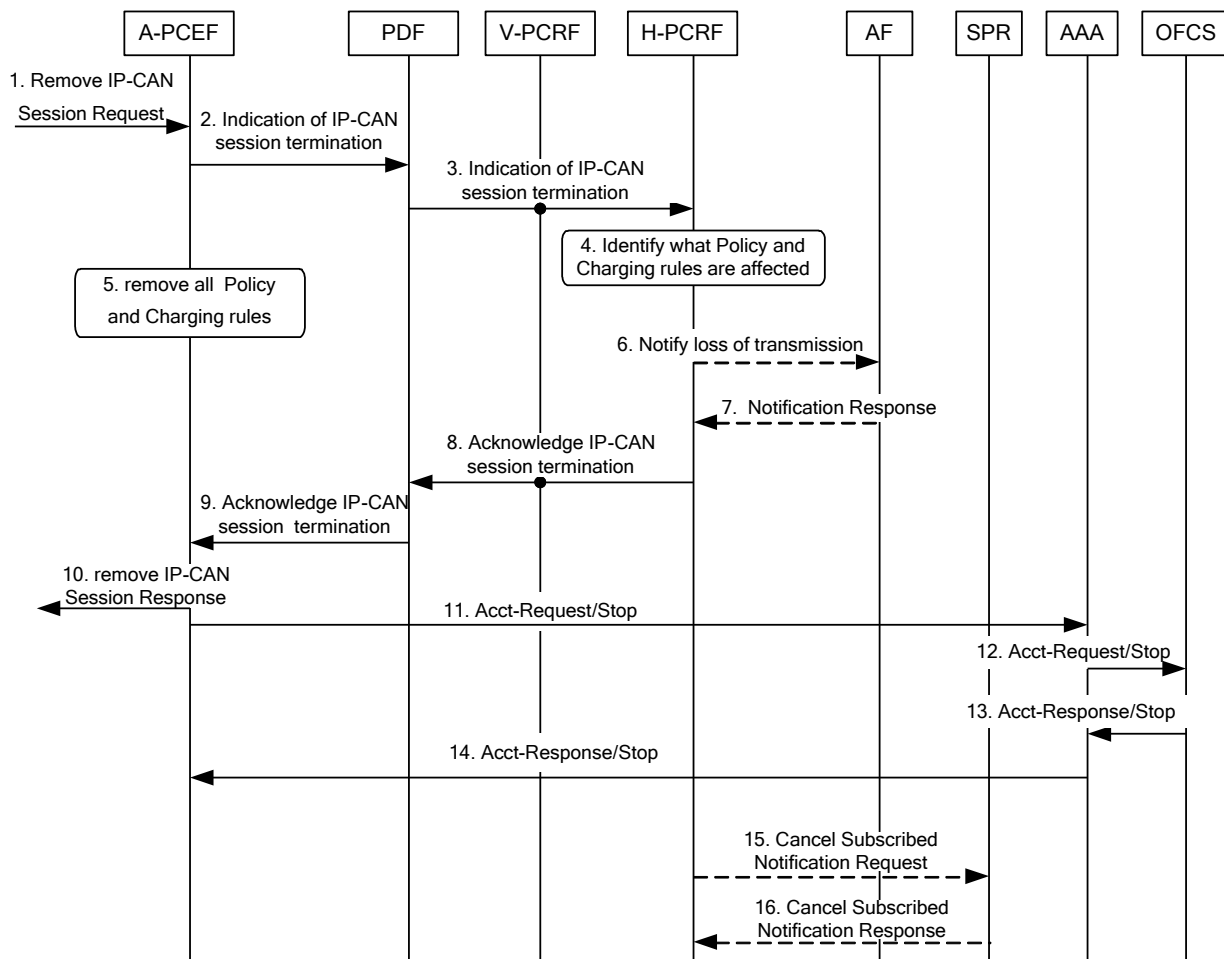


Figure 7: MS/BS initiated IP-CAN session termination

1. The A-PCEF receives either a Remove IP-CAN Session Request that requests the deactivation of the IP-CAN Session or a Remove IP-CAN Bearer request to remove the last IP-CAN bearer associated to this IP-CAN session. Remove IP-CAN Session Request is triggered due to MS/BS-initiated Network Exit or IP address release.
2. The A-PCEF indicates that the IP-CAN session is being removed and provides relevant information to PDF.
3. The PDF forwards the request with relevant information to the H-PCRF (by way of the V-PCRF in the roaming case).
4. The H-PCRF finds the PCC rules that require an AF to be notified.
5. The A-PCEF removes all PCC Rules associated with the IP-CAN session. This Step can happen paralleley anytime after Step 2.

PCC

- 1 6. The H-PCRF notifies the AF that there are no transmission resources for the service if this is
2 requested by the AF.
- 3 7. The AF acknowledges the notification of the loss of transmission resources.
- 4 8. The H-PCRF removes the information related to the terminated IP-CAN session (subscription
5 information, etc.), and acknowledges to the PDF that the H-PCRF handling of the IP-CAN session has
6 terminated (by way of the V-PCRF in the roaming case).
- 7 9. The PDF removes the information related to the terminated IP-CAN session and acknowledges
8 termination of the IP-CAN session to the A-PCEF.
- 9 10. The A-PCEF continues the IP-CAN session removal procedure. Upon completion, the A-PCEF MAY
10 remove state associated with that IP-CAN session.
- 11 11. The A-PCEF sends accounting stop message(s) to the AAA, based on the flow based accounting. The
12 accounting stop message is generated per each packet data flow and may be sent anytime after step5.
- 13 12. For offline charging, the AAA sends accounting stop message(s) to the OFCS. Steps 11-12 can be
14 performed at any time after Step 5.
- 15 13. The OFCS acknowledges the Accounting Stop Request.
- 16 14. The AAA acknowledges the Accounting Stop Request.
- 17 15. The H-PCRF sends a cancellation request to the SPR if it has subscribed such notification.
- 18 16. The SPR sends a response to the H-PCRF.
- 19 Note: The bearer termination procedure may proceed in parallel with the indication of IP-CAN Session
20 termination.

8.3.2 A-PCEF initiated Session Termination

Figure 8 is applicable if a WiMAX IP-CAN Session is being released by the A-PCEF.

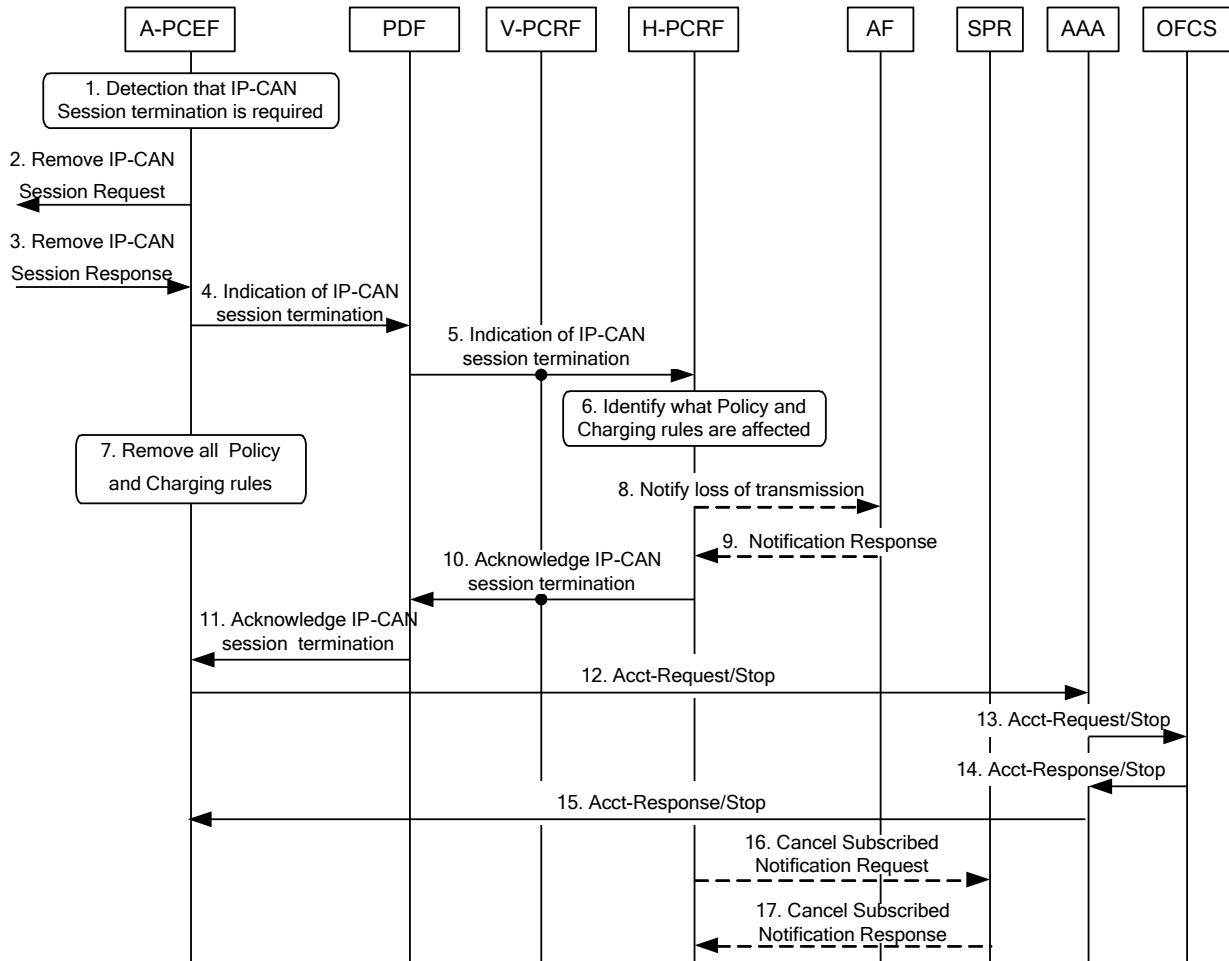


Figure 8: A-PCEF initiated IP-CAN session termination

1. The A-PCEF detects that the termination of an IP-CAN Session is required
 2. The A-PCEF sends a Remove IP-CAN Session Request message that requests the deactivation of the IP-CAN Session. This applies to each IP-CAN bearer associated to this IP-CAN session. See "Service Flow Deletion" in QoS section of [10] for the corresponding messages in the ASN.
 3. The A-PCEF receives a response to the Remove IP-CAN Session Request.
 - 4-11. Same as Steps 2-9 in Figure 7.
- Note that step 4 does not depend on completion of step 2 and 3.
- 12-17. Same as Steps 11-16 in Figure 7.
- Note: The bearer termination procedure (equivalent to the Service Flow Deletion in QoS section of [10]) may proceed in parallel with the indication of IP-CAN Session termination.

8.3.3 PCRF initiated Session Termination

Figure 9 is applicable if an IP-CAN session is being released by the PCRF.

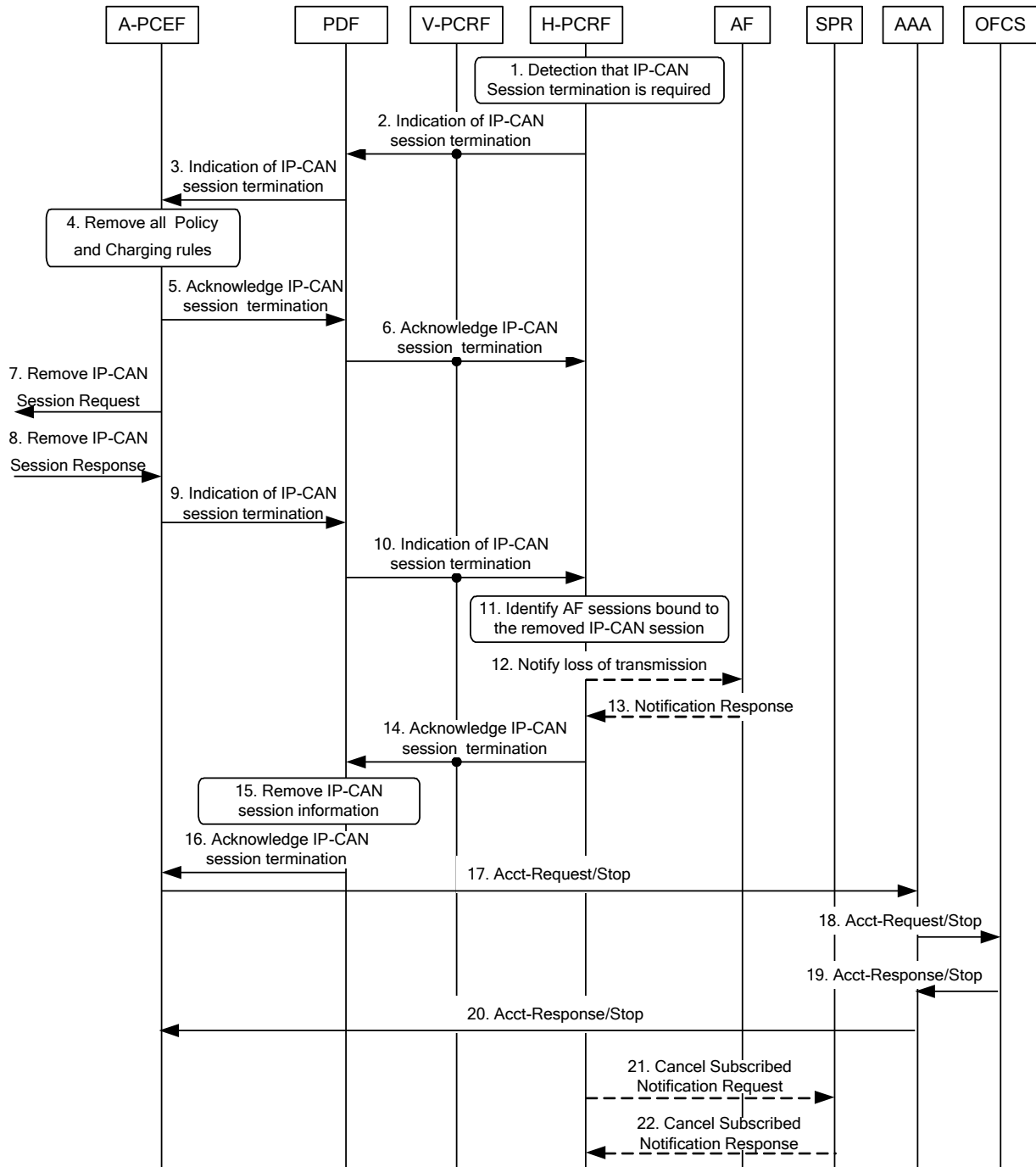


Figure 9: PCRF initiated IP-CAN session termination

1. The H-PCRF detects that the termination of an IP-CAN session is required.

PCC

- 1 2. The H-PCRF requests removal of all PCC rules previously installed for the IP-CAN session and
- 2 deactivation of all PCC rules previously activated for the IP-CAN session (by way of the V-PCRF in
- 3 the roaming case).
- 4 3. The PDF processes the information and indicates the IP-CAN Session termination to the A-PCEF.
- 5 4. The A-PCEF removes all the policy and charging rules related to the terminated IP-CAN session.
- 6 5. The A-PCEF acknowledges the session termination.
- 7 6. The PDF acknowledges the session termination to the H-PCRF (by way of the V-PCRF in the
- 8 roaming case).
- 9 7. The A-PCEF sends a Remove IP-CAN Session Request that requests the deactivation of the IP-CAN
- 10 Session.
- 11 8. The A-PCEF receives a response to the Remove IP-CAN Session Request.
- 12 9-11. Same as Steps 2-4 in Figure 7.
- 13 Note that step 9 does not depend on the outcome of step 7 and 8.
- 14 12-14. Same as Steps 6-8 in Figure 7.
- 15 15. The PDF removes the information related to the terminated IP-CAN session.
- 16 16-22. Same as Steps 11-17 in Figure 8.

17 8.4 Session modification

18 A session modification can be initiated by PCRF or A-PCEF. Following events trigger session modification:

- 19 • An AF session establishment or modification triggers PCRF initiated IP-CAN session modification.
- 20 • SPR triggered session modifications trigger PCRF initiated IP-CAN session modification.
- 21 • A service flow initiation or termination as well as change of QoS in ASN, trigger A-PCEF initiated IP-
- 22 CAN session modification.

23 Note that sleep mode and idle mode imposes no change to a WiMAX session.

24 When the session modification procedure occurs in the Non-Roaming case, the V-PCRF is not involved.

25 In the case of roaming the V-PCRF is employed to forward messages from the H-PCRF in the home network, by

26 way of the V-PCRF in the visited network to the ASN.

27 This procedure applies to the scenario where user accesses home services.

28 8.4.1 PCRF Initiated Session Modification

29 Figure 10 applies to PCRF initiated IP-CAN Session modifications.

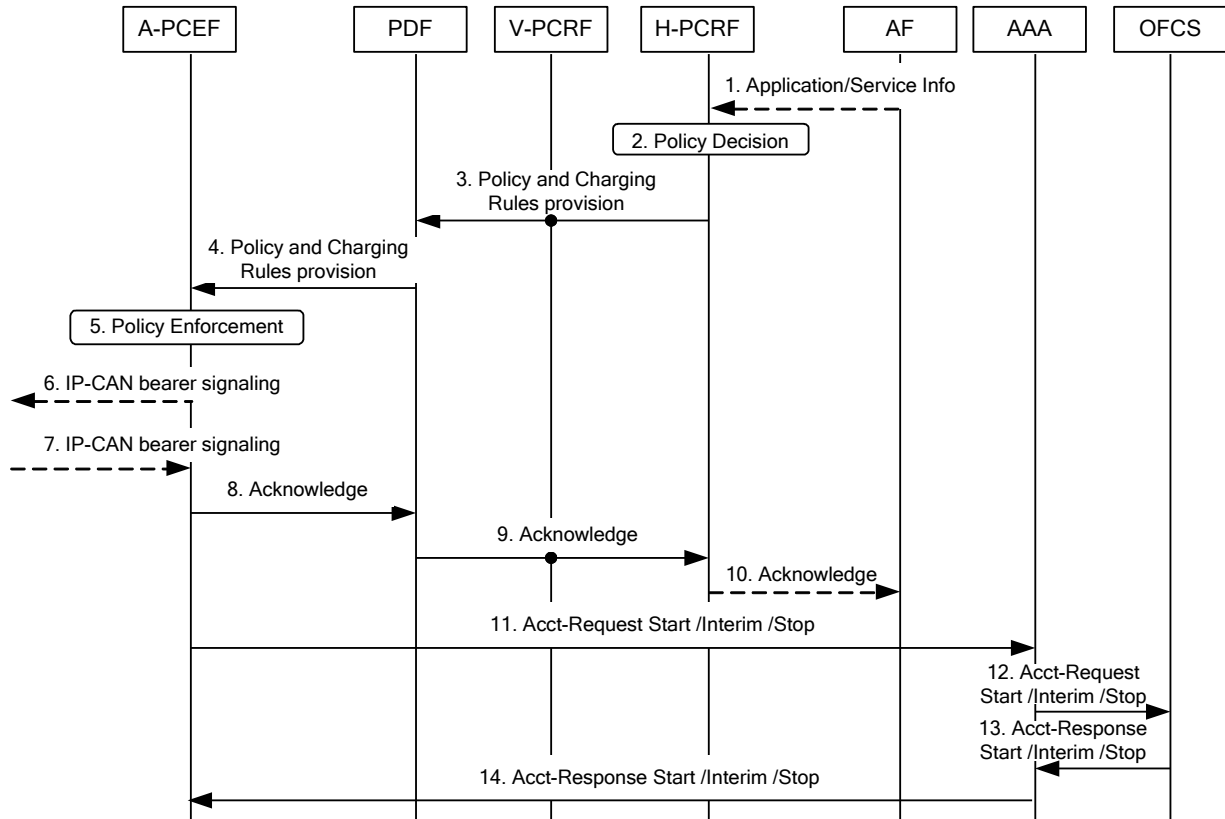


Figure 10: PCRF initiated IP-CAN session modification

1. Optionally, the AF provides service information to the H-PCRF due to AF session signalling. Optionally, without AF interaction, a trigger event in the H-PCRF may cause the H-PCRF to determine that the PCC rules require updating at the PCEF, e.g., change to configured policy.
2. The H-PCRF performs Session Binding and makes the authorization and policy decision.
3. The H-PCRF sends the decision(s) to the PDF (by way of the V-PCRF in the roaming case).
4. The PDF processes the received information and forwards the relevant information to the A-PCEF.
5. The A-PCEF enforces the decision.
6. The A-PCEF may send an IP-CAN bearer establishment, modification, or termination request to the SFA and/or SFM. An IP-CAN bearer termination request is sent by the A-PCEF if all PCC rules for an IP-CAN bearer have been removed.
7. The A-PCEF receives the response from the SFA and/or SFM for the IP-CAN bearer modification or termination request.
8. The A-PCEF sends ACK (accept or reject of the PCC decision(s)) to the PDF.
9. The PDF processes the information and sends ACK to the H-PCRF (by way of the V-PCRF in the roaming case).
10. The H-PCRF stores the service information and responds with an Acknowledgement to the AF.

PCC

11. The A-PCEF sends the accounting message(s) to the AAA. During IP-CAN session modification, if a packet data flow is generated then accounting start message is sent for each packet data flow generated. If a packet data flow is modified then accounting interim message is sent for each packet data flow modified. If a packet data flow is terminated then accounting stop message is sent for each packet data flow terminated.
12. For offline charging, the AAA sends accounting message(s) to the OFCS.
13. The OFCS acknowledges the Accounting Start/Interim/Stop Request.
14. The AAA acknowledges the Accounting Start/Interim/Stop Request.

8.4.2 SPR Triggered Session modification

Figure 11 applies to session modification due to update of the subscription information in the PCRF.

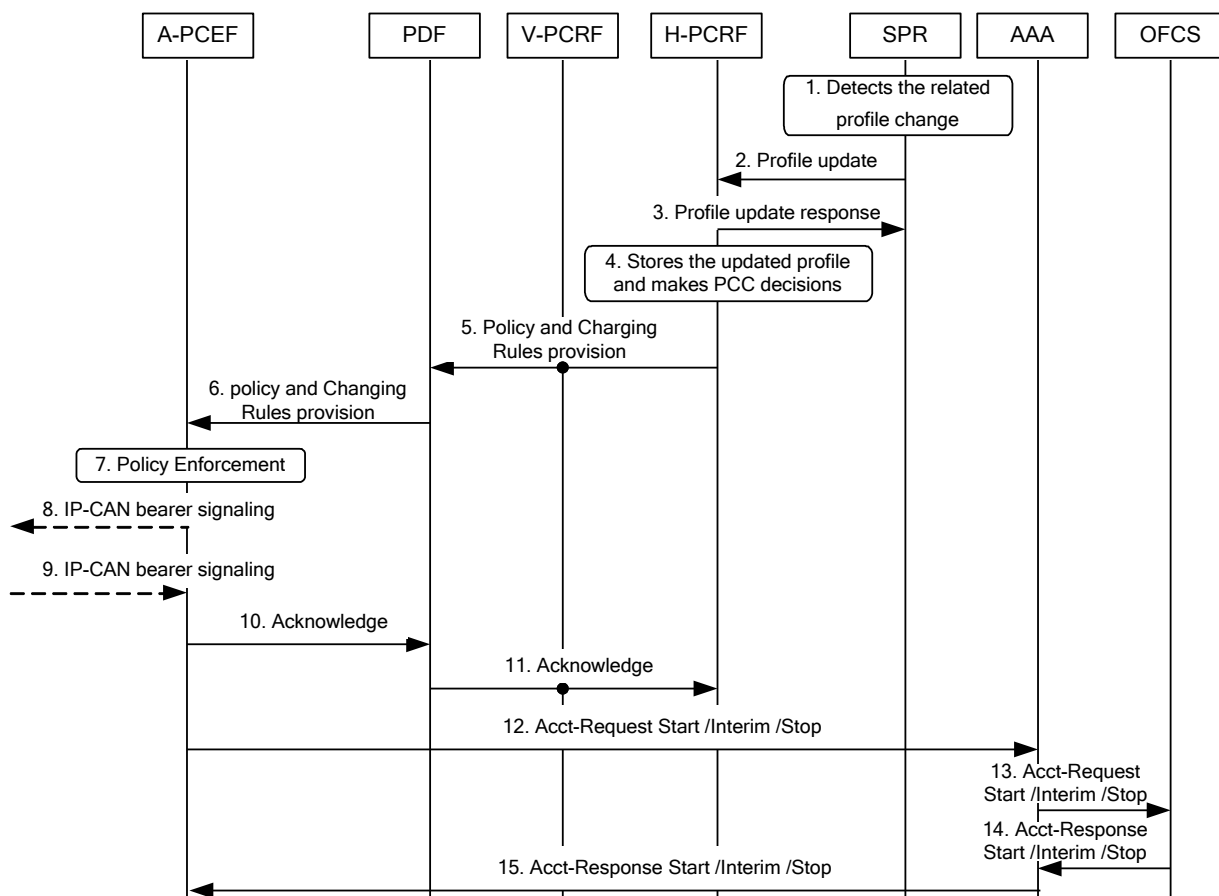


Figure 11: SPR triggered session modification

1. The SPR detects that the related subscription profile of an IP-CAN session has been changed.
2. If requested by the H-PCRF, the SPR notifies the H-PCRF on the changed profile.
3. The H-PCRF responds to the SPR.
4. The H-PCRF stores the updated profile and makes resulting PCC decisions.
- 5-11 Same as Steps 3-9 in Figure 10.
- 12-15 Same as Steps 11-14 in Figure 10.

PCC

8.4.3 A-PCEF Initiated Session Modification

This section is applicable for the establishment of a new IP-CAN bearer (other than the one which created the IP-CAN session), for the modification of an already established IP-CAN bearer and the deactivation of an IP-CAN Bearer while other IP-CAN Bearers and thus the IP-CAN Session are not released.

A bearer-event-initiated Request of PCC rules occurs when a new bearer is established or when an existing bearer is modified.

An IP-CAN Session modification triggers a PCC Rule request only if the PCRF had previously requested a PCC Rule indication for the given modification event.

Figure 12 applies to MS, BS, or A-PCEF-initiated IP-CAN bearer establishment, modification, or termination.

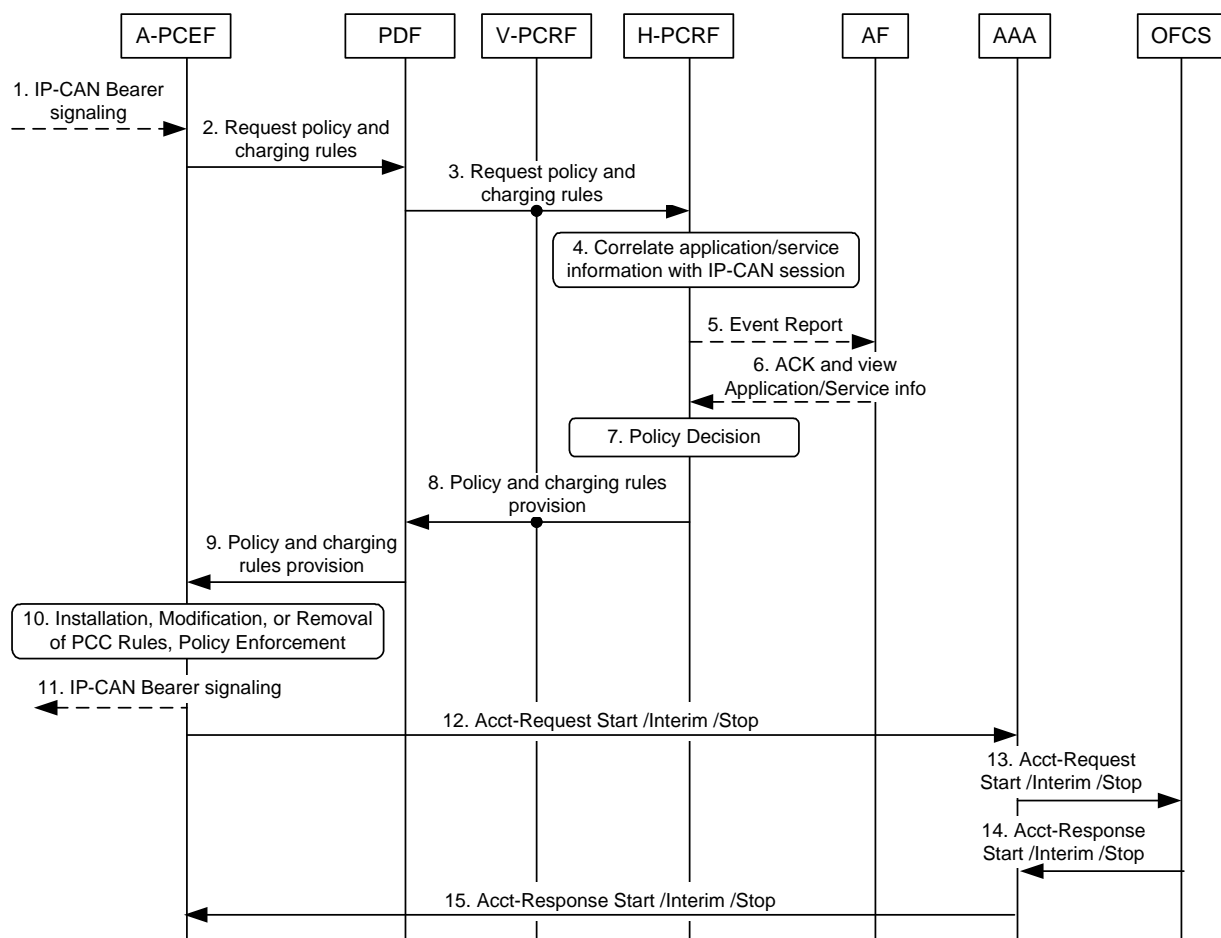


Figure 12: A-PCEF initiated IP-CAN session modification

1. The A-PCEF makes an internal decision or receives a request for IP-CAN bearer establishment, modification, or termination.
2. The A-PCEF determines that the PCC interaction is required and sends the PCC rule request to the PDF. If there is a limitation or termination of the transmission resources for a PCC rule, the A-PCEF reports this to the PDF.
3. The PDF process the information and forwards the relevant information to the H-PCRF (by way of the V-PCRF in the roaming case).

PCC

4. The H-PCRF correlates the request for PCC rules with the IP-CAN session and service information available at the A-PCEF.
5. The H-PCRF may need to report to the AF an event related to the transmission resources and/or if the AF requested at initial authorisation or if the H-PCRF requires more information from the AF before authorising the network resources modification.
6. The AF acknowledges the event report and/or responds with the requested information.
7. The H-PCRF makes the authorization and policy decision.
8. The H-PCRF sends the decision(s) to the PDF (by way of the V-PCRF in the roaming case).
9. The PDF processes the information and sends the decision(s) to the A-PCEF.
10. The A-PCEF enforces the decision(s).
11. The A-PCEF acknowledges or rejects any IP-CAN bearer signalling received in Step 1.
Note: Based on the PCC rules provided by the PDF and A-PCEF bearer binding decisions, the A-PCEF may send additional IP-CAN bearer establishment, modification, or termination request to the SFA and/or SFM. An IP-CAN bearer termination request is sent by the A-PCEF if the PCC rule for an IP-CAN bearer has been removed.
- 12-15. Same as Steps 11-14 in Figure 10.

8.5 Handling mobility

8.5.1 A-PCEF relocation

Figure 13 is applicable if A-PCEF relocation, i.e., Anchor SFA relocation, is completed as a result of reauthentication with authenticator relocation and Serving SFA relocation when Serving SFA is colocated with Anchor SFA.

PCC

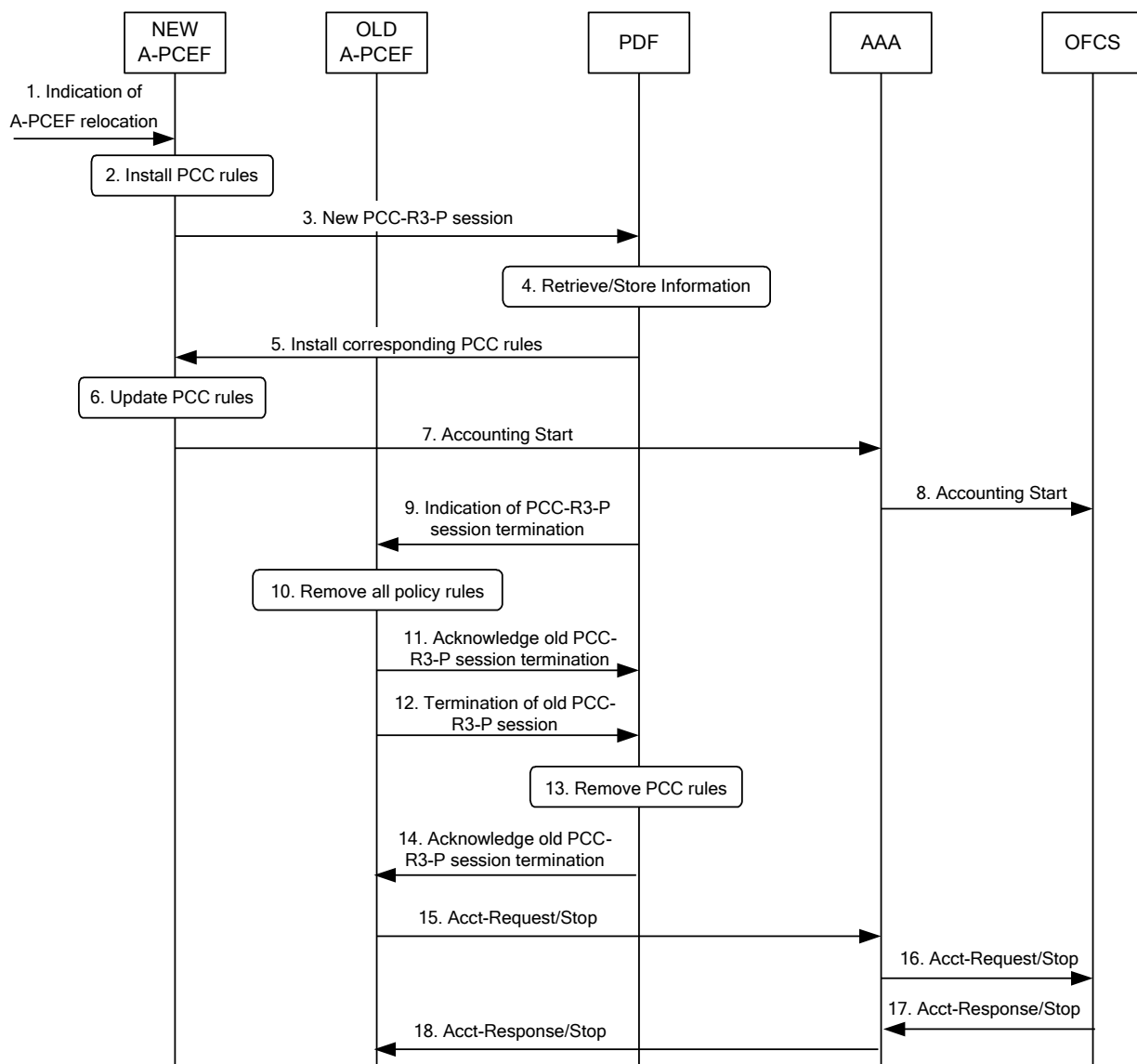


Figure 13: A-PCEF relocation

1. The new A-PCEF receives an Indication of a successful completion of reauthentication with authenticator relocation, including an MS context transfer. The MS context includes active PCC rules, their mapping into WiMAX Service Flows and associated SF parameters, as well as the PDF's identity (to be used by the new A-PCEF).
2. The new A-PCEF installs the PCC rules received during the context transfer.
3. The new A-PCEF informs the PDF of the A-PCEF relocation by establishing a new PCC-R3-P session with an indication of A-PCEF relocation.
 Editor's note: It is FFS whether additional information is needed in step 3 to help the PDF identify the appropriate old PCC-R3-P that has been relocated.
4. The PDF retrieves the information from the old PCC-R3-P session and stores it in the new PCC-R3-P session. The PDF associates the existing PCRF session with the new PCC-R3-P session such that PCRF initiated requests (e.g., PCC rules resulting from AF/SPR session modification requests) are sent to the new A-PCEF.

PCC

5. The PDF installs the PCC rules that it had retrieved from the old PCC-R3-P session.
6. A-PCEF updates the rules accordingly.
7. The new A-PCEF sends accounting start message(s) for the packet data flow(s) established.
8. For offline charging, the AAA sends accounting start message(s) to the OFCS.
9. The PDF indicates the PCC-R3-P session termination to the old A-PCEF. The signalling is described in Section 8.3.3.
10. All PCC rules related to this IP-CAN session are removed in the old A-PCEF.
11. The old A-PCEF acknowledges the PCC-R3-P session termination to the PDF. The signalling is described in Section 8.3.3.
12. The old A-PCEF informs the PDF of the termination of the old PCC-R3-P session.
13. The PDF cleans up state related to the old PCC-R3-P session.
14. The PDF acknowledges the termination of the PCC-R3-P session.
15. The old A-PCEF sends accounting stop message(s) to the AAA for the removed packet data flow(s).
16. For offline charging, the AAA sends accounting stop message(s) to the OFCS.
17. The OFCS acknowledges the Accounting Stop Request.
18. The AAA acknowledges the Accounting Stop Request.

8.6 Procedures and Flows for Online Charging

Following procedures cover the case when PCC framework is present as well as when it is absent.

8.6.1 Session Establishment

8.6.1.1 Initial and Pre-Provisioned Service Flow Creation

Figure 14 depicts the message flows for initial and preprovisioned service flow creation.

PCC

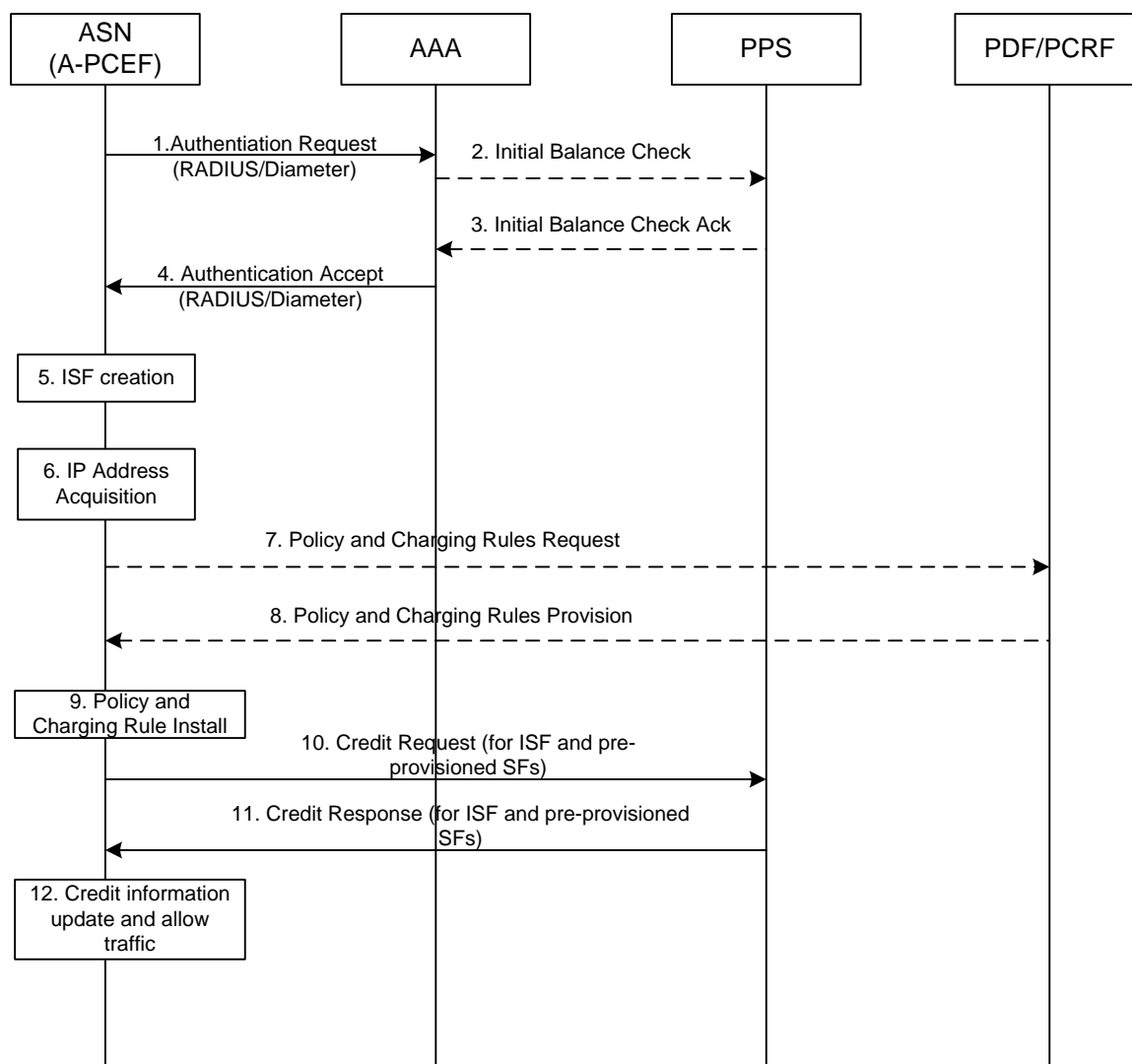


Figure 14: Initial and Pre-provisioned Service Flow Creation

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 hotlining.
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. ISF is created and resources are allocated to the MS. Optionally, pre-provisioned SFs could be created but traffic shall be blocked until PCRF authorizes traffic and PPS provides sufficient quota for the ISF/PPSF (see step 12).
6. IP address is assigned but user traffic to CSN is blocked.

PCC

- 7-8. If PCC is applicable, the ASN requests policy and charging rules for ISF and pre-provisioned SFs, and the PDF/PCRF sends these rules to the ASN.
9. Policy and charging rules are installed.
10. The ASN requests credit from the PPS for all pre-provisioned SFs and ISF.
11. The PPS returns credit to the ASN for these SFs.
12. 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.

8.6.2 Session Termination

8.6.2.1 MS/SS/BS Initiated

Figure 15 depicts the message flows for MS/SS/BS initiated session termination:

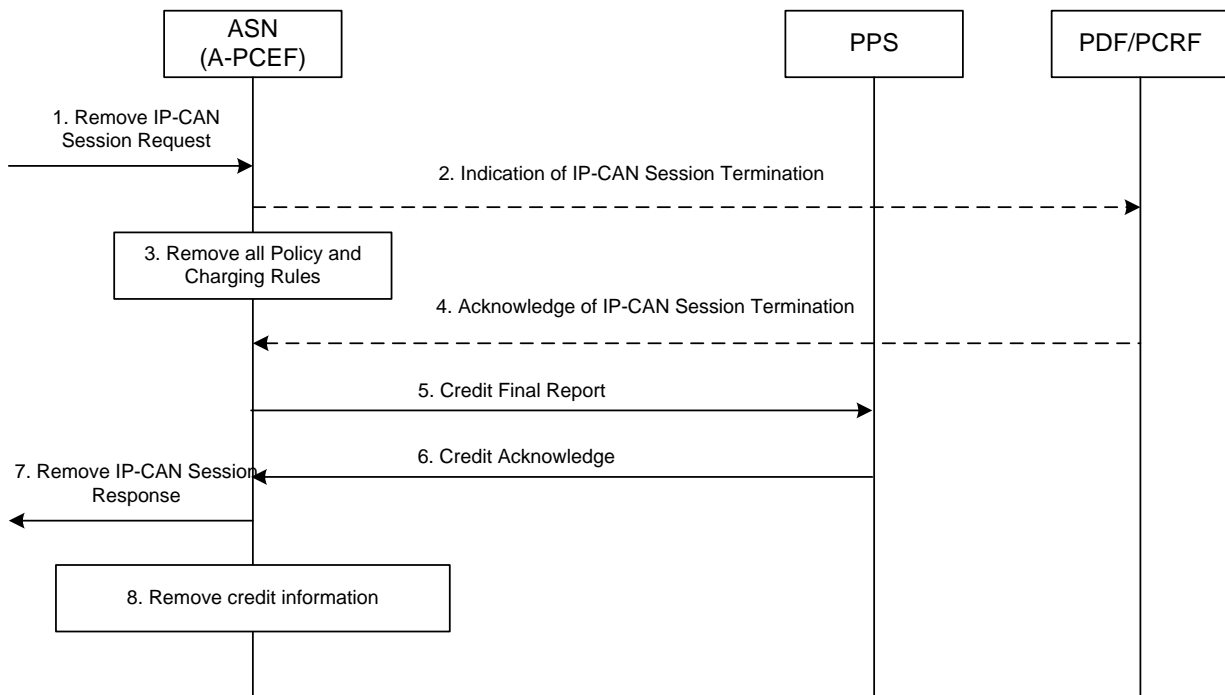


Figure 15: MS Initiated IP-CAN Session Termination

1. Same as Step 1 of section 8.3.1.
2. If PCC is applicable, the ASN indicates that the IP-CAN session is being removed and provides relevant information to PDF/PCRF.
3. ASN removes all policy and charging rules related with this IP-CAN session.
4. PDF/PCRF acknowledges to ASN the termination of the IP-CAN session.
5. ASN issues final reports and returns the remaining credit to PPS.
6. PPS acknowledges the credit report.

7. ASN continues the IP-CAN session removal procedure.
8. ASN removes all credit information of this IP-CAN session.

Note: The IP-CAN Session removal procedure may proceed in parallel with the indication of IP-CAN Session termination.

8.6.2.2 ASN Initiated

Figure 16 depicts the message flows for ASN initiated session termination:

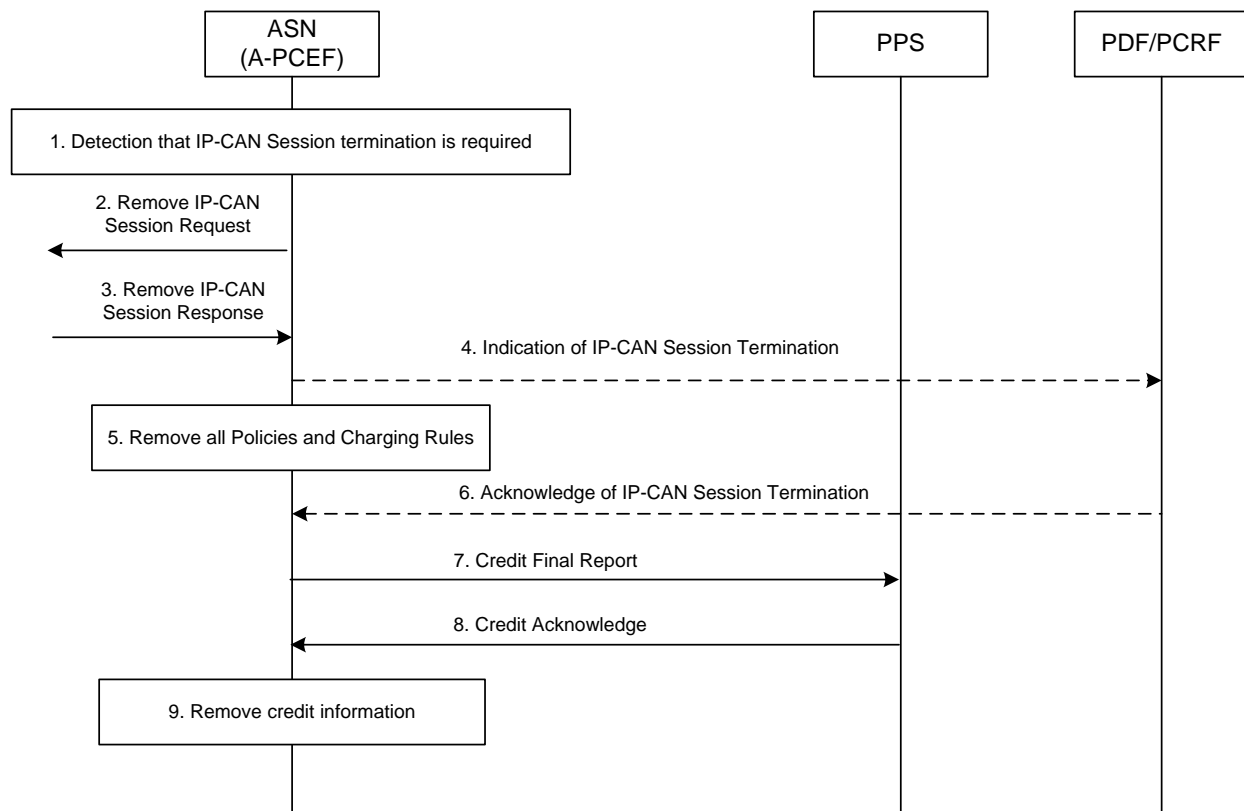


Figure 16: ASN Initiated IP-CAN Session Termination

PCC

1. The ASN detects that the termination of an IP-CAN Session is required.
2. The ASN sends a Remove IP-CAN Session Request that requests the deactivation of the IP-CAN Session. This applies to each IP-CAN bearer associated to this IP-CAN session.
3. A-PCEF/Anchor-SFA in the ASN has released all IP-CAN bearers / Service Flows related to the Session.
4. If PCC is applicable, the ASN indicates that the IP-CAN session is being removed and provides relevant information to PDF/PCRF.
5. ASN removes all policy and charging rules related with this IP-CAN session.
6. PDF/PCRF acknowledges to the ASN the termination of the IP-CAN session.
7. ASN issues final reports and returns the remaining credit to PPS.
8. PPS acknowledges the credit report.
9. ASN removes all credit information of this IP-CAN session.

Note: The IP-CAN Session removal procedure may proceed in parallel with the indication of IP-CAN Session termination.

8.6.2.3 PCRF Initiated

The message flows for PCRF initiated session termination are shown in Figure 17.

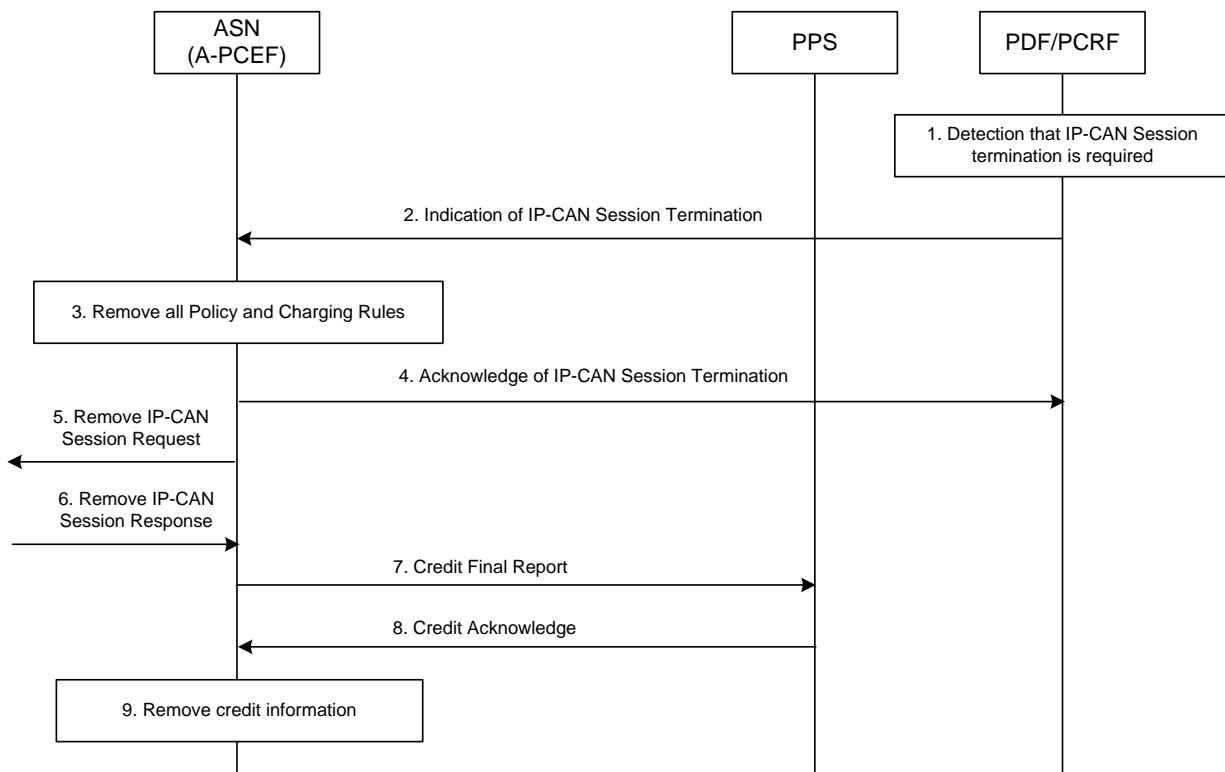


Figure 17: PCRF Initiated IP-CAN Session Termination

1. The PCRF detects that the termination of an IP-CAN session is required.
2. The PCRF requests removal of all PCC rules previously installed for the IP-CAN session and deactivation of all PCC rules previously activated for the IP CAN session.

PCC

3. ASN removes all related policy and charging rules.
4. ASN acknowledges the session termination.
5. ASN sends a Remove IP-CAN Session Request that requests the deactivation of the IP-CAN Session. It is FFS what the WiMAX Signalling for this is.
6. ASN receives a response to the Remove IP-CAN Session Request. It is FFS what the response for WiMAX is.
7. ASN issues final reports and returns the remaining credit to PPS.
8. PPS acknowledges the credit report.
9. ASN removes all credit information of this IP-CAN session.

Note: The IP-CAN Session removal procedure may proceed in parallel with the indication of IP-CAN Session termination.

8.6.3 Session Modification

8.6.3.1 PCRF Initiated

Figure 18 shows the message flows for PCRF initiated session modification:

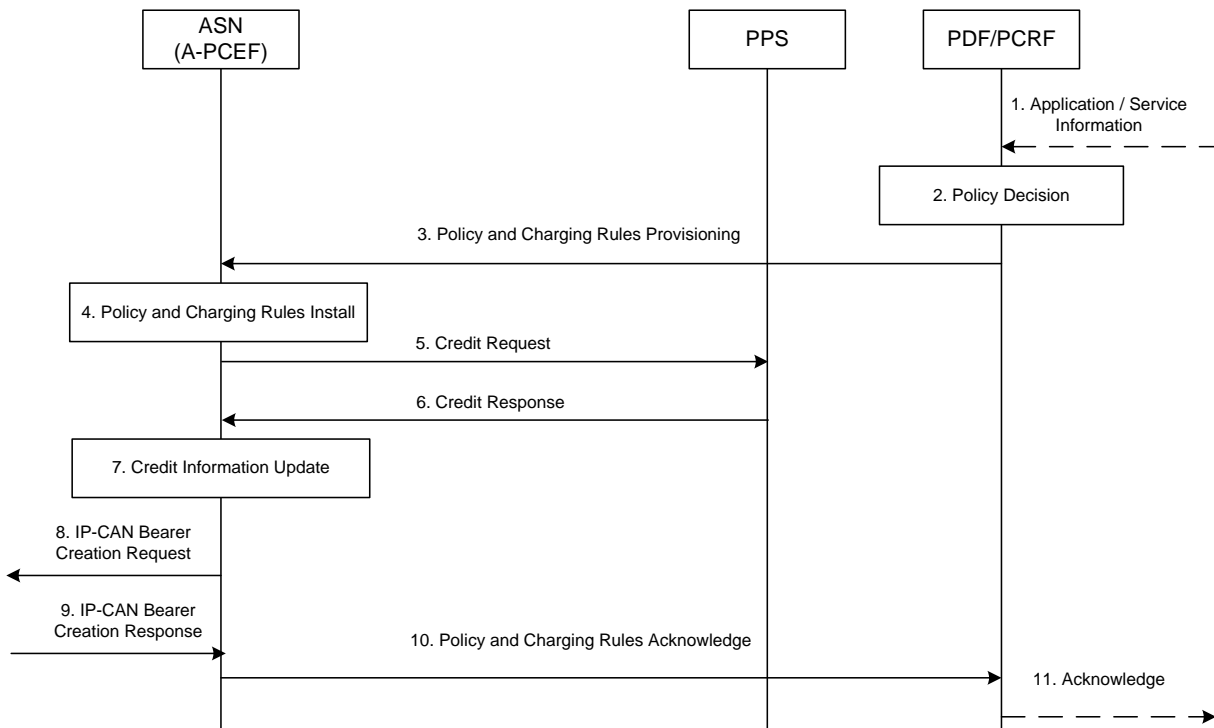


Figure 18: PCRF Initiated IP-CAN Session Modification

1. Optionally, the AF provides service information to the PDF/PCRF due to AF session signalling. Optionally, without AF interaction, a trigger event in the PDF/PCRF may cause the PDF/PCRF to determine that the PCC rules require updating at the PCEF, e.g., change to the configured policy.
2. PDF/PCRF makes the authorization and policy decision.
3. PDF/PCRF sends the decision(s) to the ASN.
4. The updated Policy and charging rules are installed.

PCC

5. ASN requests credit from PPS for all new or modified PCC rules and sends the final credit report for any deleted PCC rules.
6. PPS returns credit to ASN for new or modified rules and confirms receipt of any final reports.
7. ASN updates credit information in related policy and charging rules.
8. ASN may send an IP-CAN bearer establishment, modification, or termination request.
9. ASN receives the response for the IP-CAN bearer establishment, modification or termination request.
10. ASN sends acknowledge (accept or reject of the PCC decision(s)) to the PDF/PCRF.
11. PDF/PCRF acknowledges to the AF if necessary.

8.6.3.2 ASN Initiated

Figure 19 shows the message flows for ASN initiated session modification:

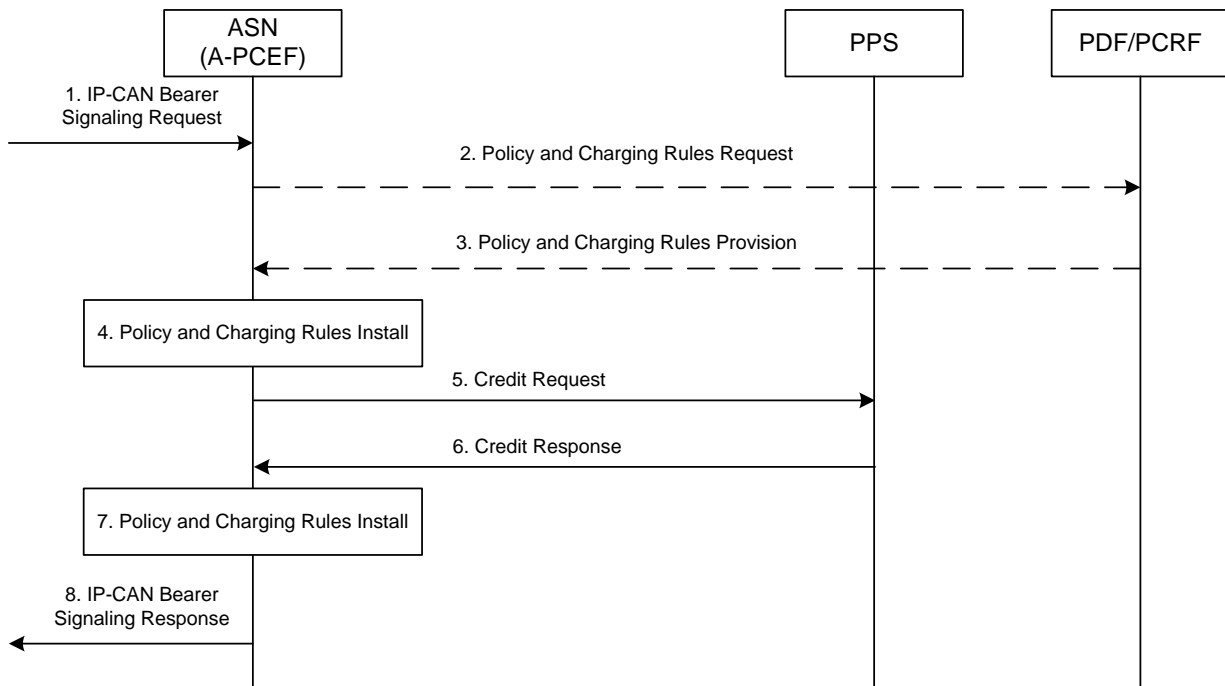


Figure 19: ASN Initiated IP-CAN Session Modification

1. ASN makes an internal decision or receives a request for IP-CAN bearer establishment, modification, or termination.
2. If PCC is applicable, ASN sends the policy and charging rule request to the PDF/PCRF.
3. PDF/PCRF makes the authorization and policy decision, and sends the updated PCC rules to the ASN.
4. The updated Policy and charging rules are installed.
5. ASN requests credit for new or modified PCC rules and sends the final credit report for any deleted PCC rules.
6. PPS returns credit to ASN for new or modified rules and confirms receipt of any final reports.
7. ASN updates the credit information in related policy and charging rules.
8. ASN continues the IP-CAN bearer modification procedure.

1 **8.6.4 Handling Mobility**

- 2 The mobility handling when the location of the PPC changes shall be done according to the Mobility Handling as
3 specified in the “PPC Relocation in case of Diameter based Online Accounting” subclause in [11].

9. Message and Parameter Definitions

9.1 PCC Framework Negotiation

Support of PCC Framework MAY be preconfigured between ASN and CSN. In this case, PCC framework should be activated for all the MSs served by the ASN (depending on ASN configuration) and per-MS negotiation during initial access authentication is not necessary.

If the above pre-configuration is not done, then PCC framework activation is negotiated between ASN, vCSN and hCSN on a per MS basis. This negotiation is performed as described below.

If ASN supports PCC framework capabilities and supports PCC framework negotiation, it SHOULD advertise this by including ASN PCC Capabilities sub-TLV in the WiMAX Capabilities VSA in the initial Access-Request message during the initial access authentication. The presence of ASN PCC Capabilities sub-TLV in the initial Access-Request indicates ASN capability to support PCC framework.

V-AAA may remove ASN indication for PCC support in the initial Access-Request message, based on vCSN policy.

H-AAA server may decide to activate PCC Framework for the specific MS when PCC Framework support capability has been advertised by the ASN and permitted by the vCSN. When deciding to activate PCC Framework for the MS, HAAA SHALL include ASN PCC Capabilities sub-TLV in WiMAX Capabilities VSA in the final Access-Accept message during initial access authentication.

9.2 PCC-R3-OC Support Negotiation

Support of PCC-R3-OC MAY be preconfigured between ASN and CSN. In this case, PCC-R3-OC support should be activated for all the subscribers served by the ASN (depending on ASN configuration). Per-subscriber negotiation during initial access authentication is not necessary.

If the above pre-configuration is not done, then PCC-R3-OC activation is negotiated between ASN, vCSN and hCSN on a per subscriber basis. This negotiation is performed as described below.

If ASN supports PCC-R3-OC capabilities and supports PCC-R3-OC negotiation, it SHOULD advertise this by including Accounting Capabilities sub-TLV with PCC-R3-OC specific value in the WiMAX Capabilities VSA in the initial Access-Request message during the initial access authentication. The presence of the Accounting Capabilities sub-TLV with PCC-R3-OC specific value in the initial Access-Request indicates ASN capability to support PCC-R3-OC.

V-AAA may remove ASN indication for PCC-R3-OC support in the initial Access-Request message, based on vCSN policy.

When deciding to activate PCC-R3-OC for the subscriber based on the configuration in subscriber's profile, HAAA SHALL include Accounting Capabilities sub-TLV with PCC-R3-OC specific value in WiMAX Capabilities VSA in the final Access-Accept message during initial access authentication.

9.2.1 Online Charging Capability Exchange with PCC Framework

Since online charging may be used by PCRF for the services of some subscribers, PCRF needs to know the online charging capability of the subscriber. The information provided by the ASN is based on ASN capabilities and AAA decision.

By including Accounting-Capabilities AVP [11] in initial CCR message from ASN to PCRF, ASN can notify PCRF the online charging capabilities supported for the subscriber to the PCRF. PCRF will decide whether it can active online charging for this MS based on the online charging capability information within Accounting-Capabilities.

9.3 Radius protocol extensions for R3 authentication

The below VSAs are added for Radius R3 Authentication reference point in order to allow support for Policy Framework.

9.3.1 ASN PCC Capabilities TLV in WiMAX Capabilities VSA

This TLV may be included by NAS in the initial Access-Request and by HAAA in the final Access-Accept during access authentication. The TLV is encapsulated in WiMAX Capabilities VSA defined in [11]:

TLV ID	TLV Name	Length Octets	AR	AA	AC	ARej
5	ASN PCC Capabilities	3	0-1[a]	0-1[b]	0	0

Notes:

- [a] The absence of this sub-TLV in an Access-Request (AR) means that the ASN (NAS) does not support Policy Framework.
- [b] The absence of this sub-TLV in an Access-Accept (AA) message means that the HAAA does not require activation of PCC Framework in ASN (IP-CAN session establishment by A-PCEF). Otherwise, if this sub-TLV is present in the Access-Accept message, this mandates PCC Framework activation in ASN for the MS.

TLV ID	5 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.

9.3.2 PCC-R3-OC Specific Value Definition

The accounting capabilities sub-TLV is defined in [11]. One value is defined for the PCC-R3-OC based accounting as following:

- 0x08 = R3-OC based accounting
- 0x10 = R3-OFC based offline accounting

Note: this information is optional as it could also be done by pre-configuration. The Access-Accept message SHALL indicate if Diameter based or RADIUS based accounting for offline or online charging shall be used.

9.4 Definition of PCC-R3-P Reference Point

To support the interworking with 3GPP/2 PCC and hide the mobility of Anchor SFA (A-PCEF), PDF is introduced in WiMAX CSN. 3GPP PCC defined Gx reference point (or 3GPP2 defined Ty reference point) is reused between PDF in the core and PCRF. However, an extension of Gx (or Ty) reference point, PCC-R3-P, is defined in WiMAX to transfer policies between the PDF and the A-PCEF. The PCC-R3-P interface enables PUSH (PDF to the A-PCEF) and PULL (A-PCEF from the PDF) mechanisms as well as handling of the relocation of A-PCEF in ASN. Here the PCC-R3-P reference point and the messages are defined. PCC-R3-P reference point utilizes DIAMETER protocol and optional RADIUS protocol. In the current specification release, the selection of RADIUS-based vs. DIAMETER-based PCC-R3-P is assumed to be preconfigured between the A-PCEF and the PDF.

9.4.1 PCC Procedures over PCC-R3-P reference point

9.4.1.1 Bearer Binding

The bearer binding is performed in the Anchor SFA/A-PCEF as defined in [2]. A PCC Rule SHOULD be bound to a single UL and DL Service Flow.

9.4.2 Diameter based PCC-R3-P Protocol

The R3 PCC protocol is based on the Gx protocol with additional optional AVPs.

With regard to the Diameter protocol defined over the PCC-R3-P interface, the PDF acts as a Diameter server, i.e., it is the network element that handles PCC Rule requests for a particular realm. The A-PCEF acts as the Diameter client, i.e., it is the network element requesting PCC rules in the transport plane network resources.

For existing AVPs predefined vendor codes are used.

For AVPs introduced by WiMAX, the WiMAX vendor ID SHALL be used.

9.4.2.1 Initialization, maintenance and termination of connection and session

The initialization and maintenance of the connection between the PDF and the A-PCEF pairs is defined by the underlying protocol. Establishment and maintenance of connections between Diameter nodes is described in RFC 3588 [18].

After establishing the transport connection, the PDF and the A-PCEF shall advertise the support of the PCC-R3-P specific Application by including the value of the WiMAX application identifier in the Auth-Application-Id AVP 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 A-PCEF and the PDF 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 [18]).

The termination of the Diameter user session is specified in RFC 3588 [18]. The description of how to use these termination procedures in the normal cases is embedded in the procedures description.

9.4.2.1.1 PCC-R3-P Auth_Application-ID

A new vendor specific Diameter Auth-Application-ID is defined for WiMAX.

The PCC-R3-P application is defined as a 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 RFC 3588 [18]) under Application IDs.

9.4.2.2 PCC-R3-P specific AVPs

PCC-R3-P is based on Gx and can be considered as an extension of it. It uses all Gx re-used AVPs (base Diameter and Diameter applications), Gx specific AVPs that are identified for All Access Types, or *WiMAX Access Type* as specified in [3]. PCC-R3-P additionally uses the optional PCC-R3-P specific AVPs defined here and listed in Table 1.

Table 1: PCC-R3-P specific AVPs

Attribute Name	AVP Code	Clause defined	Value Type (note 2)	AVP Flag rules (note 1)				May Encr.	Access type	Applicability (note 3)
				Must	May	Should not	Must not			
WiMAX-QoS-Information	407	9.4.2.2.1	Grouped	M,V	P			Y	WiMAX	Both
Packet-Size	415	9.4.2.2.3	Unsigned32	M,V	P			Y	WiMAX	Both
Packet-Interval	414	9.4.2.2.2	Unsigned32	M,V	P			Y	WiMAX	Both
Anchor-Data-Path-Address	401	9.4.2.2.4	OctetString	M,V	P			Y	WiMAX	Both
Charging-Rule-Definition	402	9.2.2.2.5	Grouped	M, V	P			Y	WiMAX	Both
WiMAX-A-PCEF-Address	411	9.2.2.2.6	Address	M,V	P			Y	WiMAX	Both
WiMAX-PCC-R3-P-Capability	404	9.4.2.2.7	Grouped	M,V	P			Y	WiMAX	Both
WiMAX-Release	301	9.4.2.2.8	OctetString	M,V	P			Y	WiMAX	Both
Accounting-PCC-R3-P-Capability	403	9.4.2.2.9	Integer32	M,V	P			Y	WiMAX	Both
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 [18].										
NOTE 2: The value types are defined in RFC 3588 [18].										
NOTE 3: AVPs marked with “CC” are applicable to charging control, AVPs marked with “PC” are applicable to policy control and AVPs marked with “Both” are applicable to both charging control and policy control.										

9.4.2.2.1 WiMAX-QoS-Information

```

WiMAX-QoS-Information ::= < AVP Header: 407 >
    [ QoS-Class-Identifier ]
    [ Max-Requested-Bandwidth-UL ]
    [ Max-Requested-Bandwidth-DL ]
    [ Guaranteed-Bitrate-UL ]
    [ Guaranteed-Bitrate-DL ]
    [ Packet Interval ]
    [ Packet Size ]

```

Note: Packet Interval and Packet Size are only relevant for uplink. DL stands for Down Link and UL for Up Link.

9.4.2.2.2 Packet-Interval AVP

The Packet-Interval AVP (AVP code 414) is of type Unsigned32 and reflects the packetization time in millisecond which should be used to calculate the polling or grant interval.

Note: The value of this parameter is based on the ptime [17].

9.4.2.2.3 Packet-Size AVP

The Packet-Size AVP (AVP code 415) is of type Unsigned32 and specifies the length in bytes of the IP Packet including the IP-header in case of IP-flows where packets have a fixed size.

9.4.2.2.4 Anchor-Data-Path-Address AVP

The Anchor-Data-Path-Address AVP (AVP code 401) is set to the IP address of the serving SFA and is included in the CCR message.

9.4.2.2.5 Charging-Rule-Definition AVP

The Charging-Rule-Definition AVP (AVP code 402) is of type Grouped, and it defines the PCC rule for a service flow sent by the PDF to the PCEF. The Charging-Rule-Name AVP uniquely identifies the PCC rule and it is used to

PCC

reference to a PCC rule in communication between the PCEF and the PDF within one IP CAN session. The Flow-Description AVP(s) determines the traffic that belongs to the service flow.

If optional AVP(s) within a Charging-Rule-Definition AVP are omitted, but corresponding information has been provided in previous PCC-R3-P messages, the previous information remains valid. If Flow-Description AVP(s) are supplied, they replace all previous Flow-Description AVP(s). If Flows AVP(s) are supplied, they replace all previous Flows AVP(s).

Flows AVP may appear if and only if AF-Charging-Identifier AVP is also present.

AVP Format:

```
Charging-Rule-Definition ::= < AVP Header: 402 >
    { Charging-Rule-Name }
    [ Service-Identifier ]
    [ Rating-Group ]
    *[ Flow-Description ]
    [ Flow-Status ]
    [ WiMAX-QoS-Information ]
    [ PDFID ]
    [ Reporting-Level ]
    [ Online ]
    [ Offline ]
    [ Metering-Method ]
    [ Precedence ]
    [ AF-Charging-Identifier ]
    *[ Flows ]
    *[ AVP ]
```

9.4.2.2.6 WiMAX-A-PCEF-Address AVP

This AVP code (411) is of type Address and indicates the IP address of the A-PCEF to the PDF.

9.4.2.2.7 Packet-Data-Flow-Info AVP

The Packet-Data-Flow-Info AVP (AVP code 405) is of type Grouped, and is used within to identify the flow being reported on. This AVP is a unique identifier within the context of an IP-CAN session for the IP flow(s) given within the same Packet-Data-Flow-Info AVP. The PDFID is discussed in section 9.8.2.4. The Flow-Description AVP(s) describe the flow represented with a specified Precedence value. This AVP is reused as defined in [3]. The Flow-Description AVP(s) supplied, replace all previous Flow-Description AVP(s). If no Flow-Description AVP is supplied, the previous values remain valid.

```
Packet-Data-Flow-Info ::= < AVP Header: 405 >
    [ PDFID ]
    [ Precedence ]
    *[ Flow-Description ]
    [ WiMAX-QoS-Information ]
    *[ AVP ]
```

9.4.2.2.7 WiMAX-PCC-R3-P-Capability AVP

This AVP code (404) is of type Grouped and identifies in a CCR message the WiMAX Capabilities supported by the ASN. In a CCA it identifies the options selected by the PCRF.

AVP Format:

```
WiMAX-PCC-R3-P-Capability ::= < AVP Header: 404 >
    { WiMAX-Release }
    [ Accounting-PCC-R3-P-Capability ]
    *[ AVP ]
```

PCC

9.4.2.2.8 WiMAX-Release AVP

The WiMAX-Release AVP (AVP code 301) as specified in [11] is of type OctetString indicating a WiMAX release formatted as: major + "." + minor. For example, the first release of WiMAX is indicated as "1.0".

Note: New versioning shall be considered.

9.4.2.2.9 Accounting-PCC-R3-P-Capability AVP

The *Accounting-PCC-R3-P-Capability* AVP (AVP code 403) is of type Enumerated and indicates the accounting capabilities in a CCR that are supported by the sender. CCA will not include this AVP.

Online	0
Offline	1
Online_and_Offline	2

9.4.2.3 PCC-R3-P Re-Used AVPs

Table 2 lists the Gx Diameter Application [3] AVPs re-used by the PCC-R3-P reference point.

Table 2: PCC-R3-P re-used Diameter AVPs

Attribute Name	Reference	Description	Access type	Applicability (note 1)
Access-Network-Charging-Address	3GPP TS 29.214 [5]	Indicates the IP Address of the network entity within the access network performing charging (e.g. the ASN/A-PCEF IP address).	All	CC
Access-Network-Charging-Identifier-Gx	3GPP TS29.212 [3]	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)	All	CC
Auth-Application-Id	IETF RFC 3588 [17]	Advertises support of the Authentication and Authorization portion of an application.	All	Both
Bearer-Control-Mode	3GPP TS29.212 [3]	Indicates who preferred bearer control mode.	All	PC
CC-Request-Number	IETF RFC 4006 [16]	The number of the request for mapping requests and answers	All	Both
CC-Request-Type	IETF RFC 4006 [16]	The type of the request (initial, update, termination)	All	Both
Charging-Information	3GPP TS 29.229 [6]	The Charging-Information AVP is of type Grouped, and contains the addresses of the charging functions in the following AVPs: <ul style="list-style-type: none"> Primary-Event-Charging-Function-Name is of type DiameterURI and defines the address of the primary online charging system. The protocol definition in the DiameterURI shall be either omitted or supplied with value "Diameter". Secondary-Event-Charging-Function-Name is of type DiameterURI and defines the address of the secondary online charging system for the bearer. The protocol definition in the DiameterURI shall be either omitted or supplied with value "Diameter". 	All	CC
Charging-Information	3GPP TS 29.229 [6]	The Charging-Information AVP is of type Grouped, and contains the addresses of the charging functions in the following AVPs: <ul style="list-style-type: none"> Primary-Charging-Collection-Function-Name is of type DiameterURI and defines the address of the primary offline charging system for the bearer. For Diameter on PCC-R3-OFC (A-PCEF – AAA) interface the protocol definition in the DiameterURI shall be either omitted or supplied with value "Diameter". Secondary-Charging-Collection-Function-Name is of type DiameterURI and defines the address of the secondary offline charging system for the bearer. For Diameter on the PCC-R3-OFC (A-PCEF – AAA) interface the protocol definition in the DiameterURI shall be either omitted or supplied with value 	All	CC

PCC

Attribute Name	Reference	Description	Access type	Applicability (note 1)
		"Diameter".		
Charging-Rule-Install	3GPP TS29.212 [3]	Used to activate, install or modify PCC rules as instructed from the PCRF to the PCEF.	All	Both
Charging-Rule-Remove	3GPP TS29.212 [3]	Used to deactivate or remove PCC rules from an IP CAN session.	All	Both
Charging-Rule-Report	3GPP TS29.212 [3]	Used to report the status of a PCC rule	All	Both
Destination-Host	IETF RFC 3588 [17]	DiameterIdentity of the destination host.	All	Both
Destination-Realm	IETF RFC 3588 [17]	Realm the message is to be routed to.	All	Both
Error-Message	IETF RFC 3588 [17]	Result-Code as a human readable error message.	All	Both
Error-Reporting-Host	IETF RFC 3588 [17]	Identity of the Diameter host that sent the Result-Code.	All	Both
Experimental-Result	IETF RFC 3588 [17]	Indicates whether a particular vendor-specific request was completed successfully or whether an error occurred.	All	Both
Failed-AVP	IETF RFC 3588 [17]	Provides debugging information in cases where a request is rejected or not fully processed due to erroneous information.	All	Both
Framed-IP-Address	IETF RFC 4005 [15]	The IPv4 address allocated for the user.	All	Both
Framed-IPv6-Prefix	IETF RFC 4005 [15]	The IPv6 address prefix allocated for the user. The encoding of the value within this Octet String type AVP shall be as defined in IETF RFC 3162 [15], Clause 2.3. The "Reserved", "Prefix-Length" and "Prefix" fields shall be included in this order.	All	Both
Guaranteed-Bitrate-UL	3GPP TS29.212 [3]	Indicates the guaranteed bitrate in bits per second for an uplink service data flow	All	PC
Guaranteed-Bitrate-DL	3GPP TS29.212 [3]	Indicates the guaranteed bitrate in bits per second for a downlink service data flow	All	PC
IP-CAN-Type	3GPP TS29.212 [3]	Indicate the type of Connectivity Access Network in which the user is connected.	All	Both
Offline	3GPP TS29.212 [3]	Defines whether the offline charging interface from the PCEF for the associated PCC rule shall be enabled.	All	CC
Online	3GPP TS29.212 [3]	Defines whether the online charging interface from the PCEF for the associated PCC rule shall be enabled	All	CC
Origin-Host	IETF RFC 3588 [17]	Identifies the endpoint that originated the Diameter message.	All	Both
Origin-Realm	IETF RFC 3588 [17]	Realm of the originator of any Diameter message.	All	Both
Origin-State-Id	IETF RFC 3588 [17]	Monotonically increasing value that is advanced whenever a Diameter entity restarts with loss of previous state.	All	Both
Precedence	3GPP TS29.212 [3]	Defines the precedence of a PCC rule in case of overlapping PCC rules.	All	Both
Proxy-Info	IETF RFC 3588 [17]	Identifies a proxy and related state information.	All	Both
QoS-Class-Identifier	3GPP TS29.212 [3]	Identifies a set of IP-CAN specific QoS parameters that define the authorized QoS	All	PC

Attribute Name	Reference	Description	Access type	Applicability (note 1)
Re-Auth-Request-Type	IETF RFC 3588 [17]	Inform the client of the action expected upon expiration of the Authorization-Lifetime.	All	Both
Result-Code	IETF RFC 3588 [17]	Provides the result code.	All	Both
Route-Record	IETF RFC 3588 [17]	Contains the identity of the peer the request was received from.	All	Both
Session-Id	IETF RFC 3588 [17]	Identifies messages related to a specific session.	All	Both
Max-Requested-Bandwidth-UL	3GPP TS 29.214 [4]	Defines the maximum authorized bandwidth for uplink.	All	PC
Max-Requested-Bandwidth-DL	3GPP TS 29.214 [4]	Defines the maximum authorized bandwidth for downlink.	All	PC
Flow-Description	3GPP TS 29.214 [4]	Defines the service flow filter parameters for a PCC rule (uplink or downlink)	ALL	PC
Network-Request-Support	3GPP TS29.212 [3]	Indicates the UE and network support of the network requested bearer control mode.	All	PC
Subscription-Id	IETF RFC 4006 [16]	The identification of the subscription (IMSI, MSISDN, etc). In WiMAX, it is set to MS "outer" NAI used during Initial access authentication.	All	Both
Termination-Cause	IETF RFC 3588 [17]	Indicate the reason why a session was terminated on the access device.	All	Both
User-Equipment-Info	IETF RFC 4006 [16]	The identification and capabilities of the terminal (IMEISV, etc.). In WiMAX, User-Equipment-Info-Type AVP should be set to value "1" indicating MAC address and User-Equipment-Info-Value AVP should be set to MSID value (MS MAC address).	All	Both
Session-Release-Cause	3GPP TS29.212 [3]	Determines the cause of release of the IP-CAN session at the PCRF	All	Both
NOTE 1: AVPs marked with "CC" are applicable to charging control, AVPs marked with "PC" are applicable to policy control and AVPs marked with "Both" are applicable to both charging control and policy control.				

9.4.2.3.1 PCC-R3-P Re-used AVPs with WiMAX specific values

9.4.2.3.1.1 Event-Trigger AVP

WiMAX adds the following triggers to the list enumerated values of the Event-Trigger-AVP defined in [3].

A-PCEF_RELOCATION (n)

This value SHALL be used whenever the PCC-R3-P terminating point changes as a result of A-SFA relocation.

Anchor_Data_Path_Change (n+1)

This value SHALL be used when the policy enforcement point changes due to Serving SFA relocation.

PCC_RULE_REAUTHORIZATION (n+2)

This value is used when the PCEF finds any suspicious PCC rules or IP-CAN sessions to be re-authorized by the PCRF/PCRF. Finding suspicious PCC information is outside the scope of this document and it is optional to implement.

PCC

9.4.2.3.1.2 Charging-Rule-Install AVP

The Charging-Rule-Install AVP is reused as defined in [3].

As WiMAX performs bearer binding only in the A-PCEF, Bearer-Identifier AVP SHALL NOT be present.

The layout of the modified AVP is as follows:

```
Charging-Rule-Install ::= < AVP Header: 1001 >
                        *[ Charging-Rule-Definition ]
                        *[ Charging-Rule-Name ]
                        *[ Charging-Rule-Base-Name ]
                        *[ AVP ]
```

Note: The Charging-Rule-Definition AVP contains the AF-Charging-Identifier used by the A-PCEF/Accounting Client to assign the value to the WiMAX SDFID attribute. See 9.4.3 for more details.

9.4.2.3.1.3 IP-CAN-Type AVP

The IP-CAN-Type AVP is reused as defined in [3]. Its value SHALL be set to “WiMAX” (3).

9.4.2.3.1.4 Access-Network-Charging-Address AVP

The Access-Network-Charging-Address AVP (AVP code 501) [5] is of type Address, and it indicates the IP Address of the network entity within the access network performing charging (e.g. A-PCEF IP address). In WiMAX, the Access-Network-Charging-Address is the address of A-PCEF (NAS-ID). The Access-Network-Charging-Address AVP SHOULD NOT be forwarded over an inter-operator interface.

9.4.2.3.1.5 Access-Network-Charging-Identifier-Gx AVP

Access-Network-Charging-Identifier-Gx as specified in 3GPP TS29.212 [3] is defined as following:

```
Access-Network-Charging-Identifier-Gx ::= < AVP Header: 1022 >
                                         { Access-Network-Charging-Identifier-Value }
                                         *[Charging-Rule-Base-Name]
                                         *[Charging-Rule-Name]
```

The AVP contains the Access-Network-Charging-Identifier-Value along with the related PCC rules names. 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.

9.4.2.3.1.6 Subscription-ID AVP

The subscription-ID AVP is used to identify the subscriber’s authentication session and is used as defined in IETF RFC 4006 [16]. The Subscription-ID AVP is set to the outer NAI used during WiMAX access authentication. In case of a pseudo-NAI, the ASN-GW SHALL always use the initial NAI which was used at the initial access-authentication while the network entry. This is necessary, as the PCRF will not be informed regarding an update of the pseudo-NAI caused by a re-authentication.

9.4.2.4 PCC-R3 Messages**CC-Request (CCR) Command**

The CCR command, indicated by the Command-Code field set to 272 and the ‘R’ bit set in the Command Flags field, is sent by the A-PCEF to PDF in order to request (or PULL) PCC rules for a bearer. The CCR command is also sent by A-PCEF to the PDF in order to indicate PCC rule related events or the termination of the WiMAX IP-CAN session. This command is used for the Request Policy and Charging Rules indicated in section 8.4.2

Message Format:

PCC

```

1  <CC-Request> ::= < Diameter Header: 272, REQ, PXY >
2      < Session-Id >
3      { Auth-Application-Id }
4      { Origin-Host }
5      { Origin-Realm }
6      { Destination-Realm }
7      { CC-Request-Type }
8      { CC-Request-Number }
9      [ Destination-Host ]
10     [ Origin-State-Id ]
11     * [ Subscription-Id ]
12     [ Bearer-Control-Mode ]
13     [ Framed-IP-Address ]
14     [ Framed-IPv6-Prefix ]
15     [ IP-CAN-Type ]
16     [ Termination-Cause ]
17     [ User-Equipment-Info ]
18     [ WiMAX-A-PCEF-Address ]
19     * [ Packet-Data-Flow-Info ]
20     [ WiMAX-PCC-R3-P-Capability ]
21     [ Access-Network-Charging-Address ]
22     [ Access-Network-Charging-Identifier-Gx ]
23     [ Anchor-Data-Path-Address ]
24     [ Bearer-Usage ]
25     * [ Charging-Rule-Report ]
26     * [ Event-Trigger ]
27     * [ Proxy-Info ]
28     * [ Route-Record ]
29     * [ AVP ]

```

30 **CC-Answer (CCA) Command**

31 The CCA command, indicated by the Command-Code field set to 272 and the 'R' bit cleared in the Command Flags
 32 field, is sent by the PDF to the A-PCEF in response to the CCR PULL command. It is used to provision PCC rules
 33 and event triggers for the bearer. The primary and secondary CCF and/or primary and secondary OCS addresses
 34 may be included in the initial provisioning. This command is used for the Policy and Charging Rules provision
 35 indicated in sections 8.4.1.1 and 8.4.2

36 Message Format:

```

37 <CC-Answer> ::= < Diameter Header: 272, PXY >
38     < Session-Id >
39     { Auth-Application-Id }
40     { Origin-Host }
41     { Origin-Realm }
42     [ Result-Code ]
43     [ Experimental-Result ]
44     { CC-Request-Type }
45     { CC-Request-Number }
46     [ Bearer-Control-Mode ]
47     * [ Event-Trigger ]
48     [ Origin-State-Id ]
49     [ WiMAX-PCC-R3-P-Capability ]
50     * [ Charging-Rule-Remove ]
51     * [ Charging-Rule-Install ]
52     [ Charging-Information ]
53     [ Online ]
54     [ Offline ]
55     [ Error-Message ]
56     [ Error-Reporting-Host ]
57     * [ Failed-AVP ]
58     * [ Proxy-Info ]
59     * [ Route-Record ]

```

PCC

1 *[AVP]

3 **Re-Auth-Request (RAR) Command**

4 The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field,
5 is sent by the PDF to the A-PCEF in order to provision PCC rules using the PUSH procedure to initiate the
6 provision of unsolicited PCC rules.

7 Message Format:

```
8  <RA-Request> ::= < Diameter Header: 258, REQ, PXY >
9      < Session-Id >
10     { Auth-Application-Id }
11     { Origin-Host }
12     { Origin-Realm }
13     { Destination-Realm }
14     { Destination-Host }
15     { Re-Auth-Request-Type }
16     [ Origin-State-Id ]
17     [ Session-Release-Cause ]
18     *[ Event-Trigger ]
19     *[ Charging-Rule-Remove ]
20     *[ Charging-Rule-Install ]
21     *[ Proxy-Info ]
22     *[ Route-Record ]
23     *[ AVP]
```

24 **Re-Auth-Answer (RAA) Command**

25 The RAA command, indicated by the Command-Code field set to 258 and the 'R' bit cleared in the Command Flags
26 field, is sent by the A-PCEF to the PDF in response to the RAR command.

27 Note: Subsequent adaptations at the ASN of parameters requested by the PCRF are reported back by a CCR
28 messages as shown in the Stage-3 message flows of TS29.213 [4].

29 Message Format:

```
30  <RA-Answer> ::= < Diameter Header: 258, PXY >
31      < Session-Id >
32      { Origin-Host }
33      { Origin-Realm }
34      [ Result-Code ]
35      [ Experimental-Result ]
36      [ Origin-State-Id ]
37      [ Event-Trigger ]
38      *[ Charging-Rule-Report ]
39      [ Access-Network-Charging-Address ]
40      *[ Access-Network-Charging-Identifier-Gx ]
41      [ Error-Message ]
42      [ Error-Reporting-Host ]
43      *[ Failed-AVP ]
44      *[ Proxy-Info ]
45      *[ AVP ]
```

46 **9.4.3 Radius based PCC-R3-P Protocol**

47 This section defines usage of RADIUS messages, attributes and VSAs for RADIUS-based PCC-R3-P reference
48 point according to the procedures described in Section 8.

49 RADIUS based PCC-R3-P protocol makes use of standard Radius attributes, WiMAX VSAs specified in the scope
50 of WiMAX Rel.1 [11] and new WiMAX VSAs designed specifically to support PCC framework.

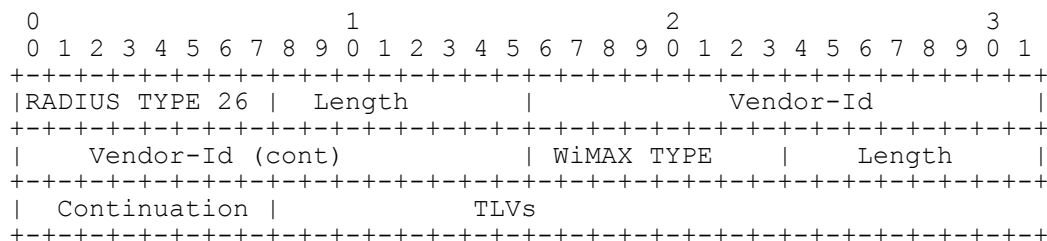
PCC

With regard to the Radius protocol defined over PCC-R3-P, the PDF acts as a Radius server and the A-PCEF acts as a Radius client. The interactions between the A-PCEF and the PDF may be either solicited or unsolicited. In the solicited mode, the A-PCEF requests the PDF to send policies and charging rules for a session/flow being established/modified in the ASN. In the unsolicited mode, the PDF pushes policies and charging rules to the A-PCEF in the unsolicited manner.

9.4.3.1 PCC-R3-P specific Radius VSAs

This section defines the new WiMAX Policy Framework specific VSAs for RADIUS-based PCC-R3-P reference point. The usage of these VSAs is presented in Section 9.4.3.3.8.

9.4.3.1.1 Access-Network-Charging-Identifier



WType-ID	200
Description	This VSA is sent by the A-PCEF to the PDF. It contains a charging identifier (PDFID for WiMAX) within the Access-Network-Charging-Identifier-Value and the related PCC rule name within either Charging-Rule-Name or Charging-Rule-Base-Name TLV. If the IP-CAN session contains only a single bearer, no Charging-Rule-Name or Charging-Rule-Base-Name needs to be provided. Otherwise, corresponding PCC rule name shall be included.
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	COA	COA-ACK
1	Access-Network-Charging-Identifier-Value	2+Length	0-1	0	0	0-1
2	Charging-Rule-Name	2+Length	0-1	0	0	0-1
3	Charging-Rule-Base-Name	2+Length	0-1	0	0	0-1

TLV ID	1 for Access-Network-Charging-Identifier-Value
Description	This TLV contains a charging identifier (PDFID for WiMAX).
Length	2+Length
Value	Octet-String

TLV ID	2 for Charging-Rule-Name
Description	This TLV provides a reference for the specific PCC rule being reported.

PCC

Length	2+Length
Value	Octet-String

TLV ID	3 for Charging-Rule-Base-Name
Description	This TLV provides a reference to a group of PCC rules predefined at the A-PCEF being reported.
Length	2+Length
Value	Text

9.4.3.1.2 Anchor-DPF-IPv4-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 | Anchor-DPF-IPv4-Address
+-----+-----+-----+-----+-----+-----+-----+-----+

```

WType-ID	201
Description	The IPv4 address of the Anchor DPF functional entity.
Length	6 + 3 + 4
Continuation	C-bit = 0
Value	Octet string containing an IPv4 address (most significant bit first)

9.4.3.1.3 Anchor-DPF-IPv6-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 | Anchor-DPF-IPv6-Address
+-----+-----+-----+-----+-----+-----+-----+-----+

```

WType-ID	202
Description	The IPv6 address of the Anchor DPF functional entity.
Length	6 + 3 + 16
Continuation	C-bit = 0
Value	Octet string containing an IPv6 address (most significant bit first)

PCC

9.4.3.1.4 Charging-Rule-Install

```

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	204
Description	This VSA is used to activate, install or modify PCC rules as instructed from the PDF to the A-PCEF. For installing a new PCC rule or modifying an already installed PCC rule, Charging-Rule-Definition TLV shall be used. For activating a PCC rule predefined at the A-PCEF, Reference-Charging-Rule-Name TLV shall be used as a reference for that PCC rule. The Charging-Rule-Base-Name TLV is a reference that may be used for activating a group of PCC rules predefined at the A-PCEF.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	One or more of the following sub-TLVs

TLV ID	TLV Name	Length Octets	AR	AA	COA	COA-ACK
1	Reference-Charging-Rule-Name	2+Length	0	0-1	0-1	0
2	Charging-Rule-Base-Name	2+Length	0	0-1	0-1	0
3	Charging-Rule-Definition	2+Length	0	0-1	0-1	0

TLV ID	1 for Reference-Charging-Rule-Name
Description	This TLV defines a name for PCC rule that is preprovisioned in the A-PCEF. It uniquely identifies a PCC rule within the A-PCEF.
Length	2+Length
Value	Octet-String

TLV ID	2 for Charging-Rule-Base-Name
Description	This TLV indicates the name of a predefined group of PCC rules residing at the A-PCEF.
Length	2+Length
Value	Text

TLV ID	3 for Charging-Rule-Definition
Description	This TLV defines the PCC rule sent by the PDF to the A-PCEF. The Charging-Rule-Name

PCC

	uniquely identifies the PCC rule and it is used as a reference to a PCC rule in communications between the A-PCEF and the PDF within one IP-CAN session. Associated PDFID provides a reference to the corresponding PDF-Descriptor VSA which includes traffic classification rules and the authorized QoS parameters. If optional TLVs within Charging-Rule-Definition are omitted, but the corresponding information has been provided in previous messages, the previous information remains valid. PDF-Descriptor parameters, referred by the Associated PDFID, replace the previously provided parameters.
Length	2+Length of TLVs
Value	The following sub-TLVs

The following TLVs appear nested within Charging-Rule-Definition TLV:

```

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   |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Charging-Rule-Name . . . . .
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

TLV ID	TLV Name	Length Octets	Occurrence
1	Charging-Rule-Name	2+Variable	1
2	Service-Identifier	2+4	0-1
3	Rating-Group	2+4	0-1
4	Charging Mode	2+1	0-1
5	AF-Charging-Identifier	2+Variable	0-1
6	Reporting-Level	2+1	0-1
7	Associated PDFID	2+2	1

TLV ID	1 for Charging-Rule-Name
Description	This TLV defines a name for PCC rule that is provided by the PDF. It uniquely identifies a PCC rule within the IP CAN session.
Length	2+Variable
Value	Octet-string.

TLV ID	2 for Service Identifier
Description	This TLV contains identifier of a service. Refer to [16].
Length	2+4
Value	Unsigned Integer.

TLV ID	3 for Rating Group
---------------	--------------------

PCC

Description	This TLV contains identifier of a rating group. Refer to [16].
Length	2+4
Value	Unsigned Integer.

1

TLV ID	4 for Charging Mode
Description	This TLV defines the charging method that should be used for the PCC rule. The absence of this TLV within the first provisioning of Charging-Rule-Definition of a new PCC rule indicates that the default charging method shall be used.
Length	2+1 octet
Value	It is of type octet bit-map. Multiple bits may be set simultaneously. The value 0 of the bit means that corresponding capability is disabled. The value 1 means that the corresponding capability is enabled. 0x01 – Offline charging (enable/ disable) 0x02 – Online charging (enable/ disable) 0x04 – Duration-based metering (enable/ disable) 0x08 – Volume-based metering (enable/ disable) Other bits are reserved.

2

TLV ID	5 for AF-Charging-Identifier
Description	This TLV contains the Application Function (AF) Charging Identifier that is sent by the AF. This information is used for charging correlation with application layer. AF-Charging-Identifier is used by the A-PCEF/ Accounting Client to assign the value to the WiMAX SDFID
Length	2+Variable
Value	Octet-String

3

TLV ID	6 for Reporting Level
Description	This TLV defines on what level the A-PCEF reports the usage of the related PCC rule.
Length	2+1
Value	Unsigned octet. 0x01 – SERVICE_IDENTIFIER_LEVEL This value shall be used to indicate that the usage shall be reported on service-id and rating group combination level. 0x02 – RATING_GROUP_LEVEL This value shall be used to indicate that the usage shall be reported on rating group level. Other values are reserved.

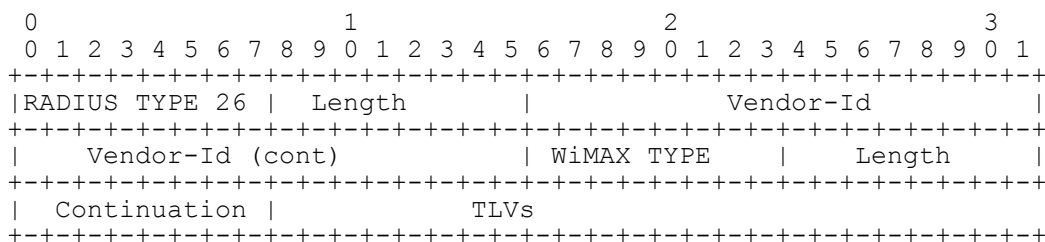
4

TLV ID	7 for Associated PDFID
Description	This TLV serves as a correlator with the corresponding PDF-Descriptor.
Length	2+2

PCC

Value	Unsigned Short representing the associated flow identifier (most significant bit first).
--------------	--

9.4.3.1.5 Charging-Info



WType-ID	203
Description	This VSA is sent by the PDF to the A-PCEF in the initial Access-Accept message and contains the addresses of the charging functions in the sub-TLVs.
Length	6 + 3 + TLVs
Continuation	C-bit = 0
Value	One or more of the following sub-TLVs

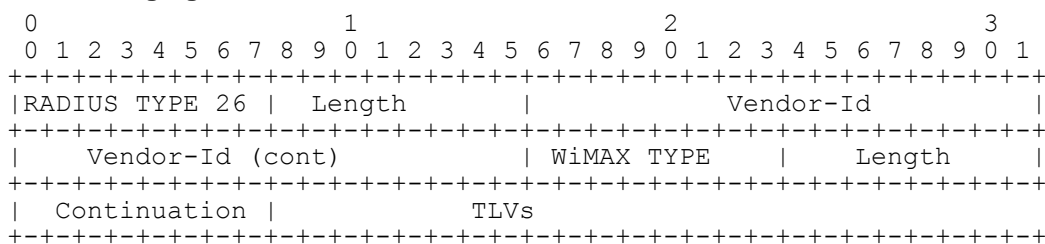
TLV ID	TLV Name	Length Octets	AR	AA	COA	COA-ACK
1	Primary-Event-Charging-Function-Name	2+Length	0	0-n	0	0
2	Secondary-Event-Charging-Function-Name	2+Length	0	0-n	0	0

TLV ID	1 for Primary-Event-Charging-Function-Name
Description	This TLV defines the address of the primary online charging system.
Length	2+Length
Value	Octet-String

TLV ID	2 for Secondary-Event-Charging-Function-Name
Description	This TLV defines the address of the secondary online charging system.
Length	2+Length
Value	Octet-String

PCC

9.4.3.1.6 Charging-Rule-Remove



WType-ID	205
Description	This VSA is used to deactivate or remove PCC rules from an IP-CAN session as instructed by the PDF to the A-PCEF.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	One or more of the following sub-TLVs

TLV ID	TLV Name	Length Octets	AR	AA	COA	COA-ACK
1	Charging-Rule-Name	2+Length	0	0-n [a]	0-n [a]	0
2	Charging-Rule-Base-Name	2+Length	0	0-n [a]	0-n [a]	0

Notes:

- [a] At least one of Charging-Rule-Name or Charging-Rule-Base-Name TLVs shall appear in the Charging-Rule-Remove VSA.

TLV ID	1 for Charging-Rule-Name
Description	This TLV provides a reference for the specific PCC rule at the A-PCEF to be removed or for the specific PCC rule preprovisioned in the A-PCEF to be deactivated.
Length	2+Length
Value	Octet-String

TLV ID	2 for Charging-Rule-Base-Name
Description	This TLV provides a reference to a group of PCC rules predefined at the A-PCEF to be deactivated.
Length	2+Length
Value	Text

PCC

9.4.3.1.7 Charging-Rule-Report

```

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	206
Description	This VSA is used to report the status of the PCC rule. It can be used to report a status of the PCC rules that cannot be installed/ activated at the A-PCEF. In this case, Charging-Rule-Name is used to indicate the specific PCC rule, which cannot be installed/ activated and the Charging-Rule-Base-Name is used to indicate a group of PCC rules which cannot be activated. A-PCEF may include Associated PDFID TLV to indicate the PDF-Descriptor and QoS-Descriptor parameters (e.g. in some event reports to indicate the affected bearer or flow classification/ QOS parameters) Multiple instances of Charging-Rule-Report VSA shall be used in the case it is required to report status of different PCC Rules.
Length	6 + 3 + TLVs
Continuation	C-bit = 0 or 1
Value	One or more of the following sub-TLVs

TLV ID	TLV Name	Length Octets	AR	AA	COA	COA-ACK	COA-NAK
1	Charging-Rule-Name	2+Length	0-1 [a]	0	0	0-1 [a]	0-1 [a]
2	Charging-Rule-Base-Name	2+Length	0-1 [a]	0	0	0-1 [a]	0-1 [a]
3	PCC-Rule-Status	2+1	0-1	0	0	0-1	0-1
4	Associated PDFID	2+2	0-1 [a]	0	0	0-1 [a]	0-1 [a]

Notes:

- [a] At least one of Charging-Rule-Name, Charging-Rule-Base-Name or Associated PDFID TLVs shall appear in the Charging-Rule-Report VSA.

TLV ID	1 for Charging-Rule-Name
Description	This TLV provides a reference for the specific PCC rule being reported.
Length	2+Length
Value	Octet-String

TLV ID	2 for Charging-Rule-Base-Name
Description	This TLV provides a reference to a group of PCC rules predefined at the A-PCEF being

PCC

	reported.
Length	2+Length
Value	Text

1

TLV ID	3 for PCC-Rule-Status
Description	This TLV describes the status of the PCC rule indicated in the Charging-Rule-Report VSA.
Length	2+1
Value	<p>Unsigned octet.</p> <p>0 – ACTIVE</p> <p>This value is used to indicate that the PCC rule is successfully installed (for those provisioned from the PDF) or activated (for those predefined in the A-PCEF).</p> <p>1 – INACTIVE</p> <p>This value is used to indicate that the PCC rule is removed (for those provisioned from the PDF) or inactive (for those predefined in the A-PCEF).</p> <p>2 – TEMPORARY_INACTIVE</p> <p>This value is used to indicate that for some reason (e.g. loss of bearer), an already installed or activated PCC rule is temporary disabled.</p> <p>Other values are reserved.</p>

2

TLV ID	4 for Associated PDFID
Description	This TLV indicates the PDFID associated with the PCC rule and may serve as a correlator with the corresponding PDF-Descriptor.
Length	2+2
Value	Unsigned Short representing the associated flow identifier (most significant bit first).

3

9.4.3.1.8 Event Trigger

```

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 | WiMAX TYPE |      Length      |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| Continuation | Event-Trigger |
+---+---+---+---+---+---+---+---+---+---+---+---+---+---+

```

14

WType-ID	207
Description	<p>This VSA is used by an A-PCEF to report ASN events that shall cause a re-request of PCC rules.</p> <p>When sent from the PDF to the PCEF, the Event-Trigger indicates an event that shall cause a re-request of PCC rules. When sent from the A-PCEF to PDF, it indicates that the corresponding event has occurred at the ASN.</p> <p>Whenever the PDF subscribes to one or more event triggers by using COA message, the A-PCEF should send a response message (COA-ACK) with relevant information (e.g.</p>

PCC

	<p>Anchor-DPF, etc.) if available and shall not include Event-Trigger VSA.</p> <p>Whenever one of these events occurs, the A-PCEF shall send the related information that has changed together with the event trigger indication.</p> <p>When the PDF sends the Event-Trigger set to NO_EVENT_TRIGGERS value, this indicates that A-PCEF shall not notify PDF of any event.</p>
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	<p>It is of type unsigned-octet:</p> <p>1 – QoS_CHANGE</p> <p>This value shall be used by the PDF in Access-Accept or COA messages to indicate that upon any QoS change (even within the limits of the current authorization) at bearer level, PCC rules shall be requested. When sent by the A-PCEF in Access-Request message, this value indicates that the A-PCEF generated the request because there has been a change in the requested QoS for a specific bearer. The PDF-Descriptor with PDFID shall be provided to indicate the affected bearer. QoS-Descriptor is required to be provided in the same request with the new values.</p> <p>2 – LOSS_OF_BEARER</p> <p>This value shall be used by the PDF in Access-Accept or COA messages to indicate that upon loss of bearer, A-PCEF should inform PDF. When sent by the A-PCEF in Access-Request message, this value indicates that the A-PCEF generated the request because the bearer associated with the PCC rules indicated by the corresponding Charging-Rule-Report VSA was lost. The PCC-Rule-Status TLV within Charging Rule Report VSA shall indicate that these PCC rules are temporarily inactive. A-PCEF may include also the associated PDFIDs (in Associated-PDFID TLVs) to indicate which bearers have been lost.</p> <p>3 – RECOVERY_OF_BEARER</p> <p>This value shall be used by the PDF in the Access-Accept or COA messages to indicate that upon recovery of bearer, A-PCEF should inform PDF. When sent by the A-PCEF in Access-Request message, this value indicates that the A-PCEF generated the request because the bearer associated with the PCC rules indicated by the corresponding Charging-Rule-Report VSA was recovered. The PCC-Rule-Status TLV within Charging Rule Report VSA shall indicate that these PCC rules are active. A-PCEF may include also the associated PDFIDs (in Associated-PDFID TLVs) to indicate which bearers have been recovered.</p> <p>4 –A-PCEF_MALFUNCTION</p> <p>This value shall be used by the PDF in Access-Accept or COA messages to indicate that upon a failure in enforcement of PCC rules due to A-PCEF malfunction, the A-PCEF should inform the PDF. When sent by the A-PCEF in Access-Request or COA-NAK messages, this value indicates that the A-PCEF generated the request or response due to a malfunction in the A-PCEF and the PCC rules cannot be enforced. The affected PCC rules will be provided in the Charging-Rule-Report VSA. A-PCEF may include also the associated PDFIDs (in Associated-PDFID TLVs).</p> <p>5 – RESOURCE_LIMITATION</p> <p>This value shall be used by the PDF in Access-Accept or COA messages to indicate that upon a failure to provide the required resources for the flows described by the PCC rules, the A-PCEF should inform the PDF. When sent by the A-PCEF in Access-Request or COA-NAK messages, this value indicates that the A-PCEF generated the request or response because of resource limitation. The affected PCC rules will be provided in the Charging-Rule-Report VSA. A-PCEF may include also the associated PDFIDs (in Associated-PDFID TLVs).</p> <p>6 – MAX_NR_BEARER_REACHED</p>

PCC

	<p>This value shall be used by the PDF in Access-Accept or COA messages to indicate that upon a failure in the enforcement of PCC rules due to the maximum number of bearers having been reached for the session, the A-PCEF should inform the PDF. When sent by the A-PCEF in Access-Request or COA-NAK messages, this value indicates that the A-PCEF generated the request or response because the PCC rules cannot be enforced since the session already contains the maximum number of bearers allowed. The affected PCC rules will be provided in the Charging-Rule-Report VSA.</p> <p>7 – QOS_CHANGE_EXCEEDING_AUTHORIZATION</p> <p>This value shall be used by the PDF in Access-Accept or COA messages to indicate that only upon a requested QoS change beyond the current authorized value(s) at bearer level, PCC rules shall be requested. When sent by A-PCEF, it indicates that there has been a change in the requested QoS beyond the authorized value(s) for a specific bearer. The PDF-Descriptor with PDFID shall be provided to indicate the affected flow. QoS information (QOS-Descriptor VSA) is required to be provided in the same request with the requested values.</p> <p>8 – NO_EVENT_TRIGGER</p> <p>This value shall be used by the PDF to indicate that it does not require any Event Trigger notification.</p> <p>9 – A-PCEF_RELOCATION</p> <p>This value shall be used when A-PCEF relocation occurs (A-PCEF is collocated with Authenticator and Anchor SFA and is relocated together with these functional entities).</p> <p>10 – ANCHOR_DPF_CHANGE</p> <p>This value shall be used when the Anchor-DPF/ Serving-SFA relocation occurs. Note, that Anchor DPF/ Serving SFA is the ASN entity which actually handles user traffic and enforces volume-based accounting policies (i.e. it resides on the data path to the MS).</p> <p>11 – AUTHORIZATION_EXPIRY</p> <p>This value shall be used when authorization time for the session (indicated by Session-Timeout attribute) expires.</p> <p>Other values are reserved.</p>
--	---

9.4.3.1.9 PCC 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	208
Description	<p>This VSA is used to negotiate PCC capabilities during IP-CAN session establishment (in the initial Access-Request/ Accept messages).</p> <p>In the initial Access-Request it identifies the PCC Capabilities supported by the ASN. In the initial Access-Accept, it identifies the options selected by the RADIUS server.</p>
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
1	Bearer Control Mode	3	0-1	0-1
2	Charging Method	3	0-1	0-1

TLV ID	1 for Bearer Control Mode
Description	<p>This TLV is used for Policy Control negotiation.</p> <p>In the initial Access-Request it describes the bearer control capabilities supported by the ASN (A-PCEF). In the initial Access-Accept, it specifies the option selected by the Radius Server (PDF).</p> <p>The omission of this TLV means that only network-initiated control mode is supported or should be activated.</p>
Length	2+1 octet
Value	<p>It is of type unsigned-octet:</p> <p>0 – UE_ONLY This value is used to indicate MS-initiated bearer control mode.</p> <p>1 – NW_ONLY This value is used to indicate network-initiated bearer control mode.</p> <p>2 – UE_NW This value is used to indicate both MS-initiated and network-initiated bearer control modes.</p> <p>Other values are reserved.</p>

TLV ID	2 for Charging Method
Description	<p>This TLV is used for negotiation of default charging method.</p> <p>In the initial Access-Request it indicates the default charging method preconfigured in the A-PCEF. The omission of this TLV in the initial Access-Request means that charging method preconfigured in the A-PCEF is not available.</p> <p>In the initial Access-Accept it indicates the default charging method (which should take precedence over the charging method preconfigured in the A-PCEF). The omission of this TLV in the initial Access-Accept means that charging method preconfigured in the A-PCEF is applicable as a default.</p>
Length	2+1 octet
Value	<p>It is of type octet bit-map. Multiple bits may be set simultaneously. The value 0 of the bit means that corresponding capability is disabled. The value 1 means that the corresponding capability is enabled.</p> <p>0x01 – Offline charging (enable/ disable)</p> <p>0x02 – Online charging (enable/ disable)</p> <p>0x04 – Duration-based metering (enable/ disable)</p> <p>0x08 – Volume-based metering (enable/ disable)</p>

PCC

	Other bits are reserved.
--	--------------------------

9.4.3.1.10 PCC Request 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 | WiMAX TYPE | Length |
+-----+-----+-----+-----+
| Continuation | PCC-Req.-Type |
+-----+-----+-----+-----+

```

WType-ID	209
Description	This VSA shall be included in all authorize-only Access-Request messages sent by A-PCEF to PDF to indicate the reason of sending the request message – i.e. whether the request message is sent for IP-CAN session establishment, modification or termination.
Length	6 + 3 + 1
Continuation	C-bit = 0
Value	<p>It is of type unsigned-octet:</p> <p>1 – Initial</p> <p>This value is used to initiate an IP-CAN session, and contains information relevant for the session initiation.</p> <p>2 – Update</p> <p>This value is used when a request is sent for already existing IP-CAN session.</p> <p>3 – Termination</p> <p>This value is used when a request is sent in order to indicate termination of the existing IP-CAN session.</p> <p>Other values are reserved.</p>

9.4.3.1.11 Subscription-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 | Subscription-Id |
+-----+-----+-----+-----+

```

WType-ID	210
Description	Provides identification of the end-user subscription. In WiMAX, it is set to MS “outer” NAI used during initial access authentication
Length	6 + 3 + Length
Continuation	C-bit = 0 or 1

PCC

Value	Text (UTF-8 string).
--------------	----------------------

<Editor's note: other Policy Framework specific VSAs are FFS.>

9.4.3.2 PCC-R3-P re-used attributes and VSAs

The table below lists standard Radius attributes and WiMAX-specific VSAs defined in the scope of [11] reused by PCC-R3-P application.

Table 3: PCC-R3-P re-used Radius attributes and VSAs

Attribute Name	Type	Reference	Applicability (note 1)
WiMAX-Session-ID	26/4	WiMAX NWG Rel.1	Both
Calling-Station-Id	31	RFC 2865	Both
Error-Cause	101	RFC 3576	PC
Framed-IP-Address	8	RFC 2865	Both
Framed-IPv6-Prefix	97	RFC 3162	Both
hHA-IP-MIP4	26/6	WiMAX NWG Rel.1	Both
hHA-IP-MIP6	26/7	WiMAX NWG Rel.1	Both
NAS-Identifier	32	RFC 2865	Both
NAS-IP-Address	4	RFC 2865	Both
NAS-IPv6-Address	95	RFC 3162	Both
Packet-Flow-Descriptor	26/ 28	WiMAX NWG Rel.1	PC
QoS-Descriptor	26/ 29	WiMAX NWG Rel.1	PC
Service-Type	6	RFC 2865	PC
Session-Timeout	27	RFC 2865	PC
Termination-Action	29	RFC 2865	PC
User-Name	1	RFC 2865	Both
NOTE 1: Attributes and VSAs marked with "CC" are applicable to charging control; marked with "PC" – to policy control and those marked with "Both" are applicable to both charging and policy control.			

9.4.3.3 Messages for Radius based PCC-R3-P

The methods and procedures defined for RADIUS version of PCC-R3-P are based on the existing RADIUS messages: authorize-only Access-Request, Access-Accept, Change-of-Authorization and Disconnect Message. The RADIUS authorize-only messages are used from the A-PCEF to the PDF. The PDF uses Change-of-Authorization and Disconnect Message in an unsolicited manner to modify/terminate the ongoing sessions.

9.4.3.3.1 Access-Request

The A-PCEF sends Access-Request to the PDF to initiate IP-CAN session operation: establishment, termination or modification and to request policy and charging rules for a session or a flow that is being established at the bearer layer. This is RADIUS Access-Request message with service-type value set to “authorize-only” and PCC-Request-Type VSA value set to indicate the corresponding operation for IP-CAN session establishment/modification/termination.

The PDF responds with Access-Accept or Access-Reject.

The initial Access-Request contains the PCC-Request-Type VSA that indicates to the PDF that this is the initial request for the session. The initial Access-Request contains also all the information necessary for user/subscription identification.

The subsequent Access-Request contains the PCC-Request-Type VSA set to indicate “Update”. It also includes the necessary attributes for session and flow identification and policy and charging rules related attributes. It also contains an Event-Trigger VSA that indicates to the PDF the reason for this request.

The final Access-Request contains PCC-Request-Type VSA set to indicate “Final”. It includes the necessary attributes for session identification.

9.4.3.3.2 Access-Accept

The PCRF/PDF sends this message to the A-PCEF in response to an Access-Request message. This message may contain the request for policy and charging rules installation/activation, modification and removal/ deactivation. Also, it may include Event-Trigger VSAs which indicate the events that should be reported to the PDF by the A-PCEF.

9.4.3.3.3 Access-Reject

The PDF sends this message to the A-PCEF in response to an Access-Request if it cannot process the request successfully. This could be due to any protocol violation or administrative reason (e.g. negative policy authorization decision). On receiving this reject message, the A-PCEF shall terminate the flow or the IP session (depending on whether this reject relates to a particular flow or a particular session).

9.4.3.3.4 Change-of-Authorization

COA message is used by the PDF to provision policy and charging rules on the A-PCEF in an unsolicited manner. The PDF sends this message to the A-PCEF to convey new or updated policy and charging rules for an ongoing session and/or flow. The A-PCEF applies the PCC rules, and depending on whether rules were successfully installed/modified/removed, sends back an ACK or a NAK message.

The PDF may include Event-Trigger VSAs in the COA message, which indicates the events that should be reported to the PDF by the A-PCEF.

9.4.3.3.5 Change-of-Authorization ACK/NAK

The A-PCEF uses these messages to respond back to the PDF upon receiving a COA message from the PDF. A COA-ACK is sent back to the PDF if the COA request has been successfully processed by the A-PCEF. Otherwise, a COA-NAK message shall be sent.

9.4.3.3.6 Disconnect Message

The PDF sends this message to the A-PCEF to request termination of an ongoing IP-CAN session in an unsolicited manner. If this message is applicable, the A-PCEF acknowledges it by an ACK message. Otherwise, it sends back a NAK message.

If DM included Service-Type attribute set to the value “authorize-only”, the A-PCEF responds back with a NAK message including Error-Cause attribute set to “request-initiated” and performs additional Access-Request/ Access-Accept round.

The A-PCEF terminates the session/flow and sends authorize-only Access-Request message with PCC-Request-Type VSA indicating to the PDF that this is the final request for the session.

9.4.3.3.7 Disconnect Message ACK/NAK

The A-PCEF uses these messages to respond back to the PDF upon receiving a Disconnect Message requesting session termination.

9.4.3.3.8 RADIUS messages and attributes usage for PCC-R3-P

Table 4 lists the Radius attributes and VSAs usage for Radius-based PCC-R3-P application.

Table 4: RADIUS Messages for PCC-R3-P

Attribute	Type	Description	Access Request	Access Accept	Access Rej.	COA	COA-ACK	COA-NAK	DM	DM-ACK	DM-NAK
Anchor-DPF-IPv4-address	26/201	The IPv4 address of the Anchor DPF functional entity.	0-1 [h]	0	0	0	0	0	0	0	0
Anchor-DPF-IPv6-address	26/202	The IPv6 address of the Anchor DPF functional entity.	0-1 [h]	0	0	0	0	0	0	0	0
Access-Network-Charging-Identifier	26/200	Contains a charging identifier (PDFID for WiMAX) within the Access-Network-Charging-Identifier-Value and the related PCC rule name within either Charging-Rule-Name or Charging-Rule-Base-Name TLV.	0-n	0	0	0	0-n	0	0	0	0
WiMAX-Session-ID	26/4	A unique identifier in the home realm for this Session as set by the HAAA.	1 [f]	0	0	1 [f]	0	0	1 [f]	0	0
Calling-Station-Id	31	Set to the MAC address in binary format of the Device (WiMAX MS/ SS)	0-1 [e]	0	0	0	0	0	0	0	0
Charging-Rule-Install	26/204	Used to activate, install or modify PCC rules as instructed from the PDF to the A-PCEF.	0	0-n	0	0-n	0	0	0	0	0
Charging-Rule-Remove	26/205	Used to deactivate or remove PCC rules from an IP-CAN session as instructed by the PDF to the A-PCEF.	0	0-1	0	0-1	0	0	0	0	0
Charging-Rule-Report	26/206	Used to report the status of the PCC rule. It can be used to report a status of the PCC rules that cannot be installed/ activated at the A-PCEF.	0-n	0	0	0	0-n	0	0	0	0

Attribute	Type	Description	Access Request	Access Accept	Access Rej.	COA	COA-ACK	COA-NAK	DM	DM-ACK	DM-NAK
Charging-Info	26/203	This VSA is sent by the PDF to the A-PCEF in the initial Access-Accept message and contains the addresses of the charging functions in the sub-TLVs.	0	0-1 [g]	0	0	0	0	0	0	0
Error-Cause	101	Error Codes [RFC3576]	0	0	0-n	0	0	0-n	0	0-n	0-n
Event-Trigger	26/207	When included in Access-Request, indicates event at the bearer layer that caused this request. When included in Access-Accept or COA messages, it indicates the events to be reported by the A-PCEF.	0-n	0-n	0	0-n	0	0-n	0	0	0
Framed-IP-Address	8	The IPv4 Address assigned to the MS/SS – used as an IP session identity together with the identity of home network where this address is allocated.	0-1 [b]	0	0	0-1 [b] [f]	0	0	0-1 [b] [f]	0	0
Framed-Ipv6-Prefix	97	The IPv6 prefix assigned to the MS/SS.	0-1 [b]	0	0	0-1 [b] [f]	0	0	0-1 [b] [f]	0	0
hHA-IP-MIP4	26/6	IPv4 address of the HA. Identifies the network where MS IP address is allocated. Used together with IP address allocated to the MS as IP session identification.	0-1 [b]	0	0	0-1 [b] [f]	0	0	0-1 [b] [f]	0	0
hHA-IP-MIP6	26/7	IPv6 of the HA. Identifies the network where MS IP address is allocated. Used together with IP address allocated to the MS as IP session identification.	0-1 [b]	0	0	0-1 [b] [f]	0	0	0-1 [b] [f]	0	0
NAS-Identifier	32	This attribute contains a string identifying the A-PCEF origination of the Access-Request. The format SHALL be the fully qualified domain name of the A-PCEF	1[a]	0	0	1 [a] [f]	0	0	1 [a] [f]	0	0

PCC

Attribute	Type	Description	Access Request	Access Accept	Access Rej.	COA	COA-ACK	COA-NAK	DM	DM-ACK	DM-NAK
NAS-IP-Address	4	NAS IP Address. For PCC transactions, it represents A-PCEF and Access Network Charging addresses.	0-1[a]	0	0	0-1 [a] [f]	0	0	0-1 [a] [f]	0	0
NAS-IPv6-Address	95	NAS-Ipv6 address.	0-1[a]	0	0	0-1 [a] [f]	0	0	0-1 [a] [f]	0	0
Packet-Flow-Descriptor	26/28	The Service Flows descriptor	0-n	0-n	0	0-n	0	0-n	0	0	0
PCC Capability	26/208	Used to negotiate PCC capabilities during IP-CAN session establishment (in the initial Access-Request/ Accept messages). In the initial Access-Request it identifies the PCC Capabilities supported by the ASN. In the initial Access-Accept, it identifies the options selected by the RADIUS server.	0-1 [h]	0-1 [g]	0	0	0	0	0	0	0
PCC-Request-Type	26/209	Shall be included in all the authorize-only Access-Request messages sent by A-PCEF to PDF to indicate the reason of sending the request message – i.e. whether the request message is sent for IP-CAN session establishment, modification or termination.	1	0	0	0	0	0	0	0	0
QoS-Descriptor	26/29	The QoS descriptor for the flows	0-n	0-n	0	0-n	0	0	0	0	0
Service-Type	6	SHOULD be set to “authorize-only”.	1	0	0	0-1 [d]	0	0-1 [d]	0-1 [d]	0	0-1 [d]
Session-Timeout	27	The maximum number of seconds of service to be provided before termination/ reauthorization of the session/ flow.	0	0-1 [c]	0	0-1 [c]	0	0	0	0	0
Subscription	26/	Provides identification of	0-1	0	0	0	0	0	0	0	0

Attribute	Type	Description	Access Request	Access Accept	Access Rej.	COA	COA-ACK	COA-NAK	DM	DM-ACK	DM-NAK
n-Id	210	the end-user subscription. In WiMAX, it is set to MS “outer” NAI used during initial access authentication									
Termination-Action	29	Indicates what action the A-PCEF should take when service is completed.	0	0-1 [c]	0	0-1 [c]	0	0	0	0	0
User-Name	1	MS outer NAI obtained during access authentication.	1	0	0	1 [f]	0	0	1 [f]	0	0

1

2 **Notes:**

- [a] NAS-ID SHOULD appear. Also either NAS-IP-Address or NAS-IPv6-Address SHOULD appear.
- [b] IPv4/ IPv6 address together with network identity where this address has been allocated (hHA-IP-MIP4/ hHA-IP-MIP6) may be used for unique IP-CAN session identification.
- [c] If used, both Session-Timeout and Termination-Action SHALL be present. Termination-Action SHALL be set to “RADIUS-Request”(1). This causes the A-PCEF to re-authorize the session/ flow when the Session-Timeout expires.
- [d] When included in a DM or COA messages, a service-type attribute with value “authorize only” indicates that the Request only contains A-PCEF and session identification attributes and that the A-PCEF should attempt reauthorization by sending an Access-Request with a Service-Type attribute set to the value “authorize only”.
- [e] MUST appear in the initial Access-Request message.
- [f] Used for identification purposes only.
- [g] MAY appear in the initial Access-Accept message.
- [h] MAY appear in the initial Access-Request message.

3

4

5 **9.5 Diameter Based Offline Charging**6 **Informative**

7 Figure 20 below shows the end to end offline charging scenario. The goal is to have one accounting stream for both
8 AAA and OFCS/PCC charging in the WiMAX domain. The A-PCEF/Accounting Client in the WiMAX network
9 performs an attribute translation of the AF-Charging-Identifier received from the AF and maps it to the WiMAX
10 SDFID (service data flow identifier) attribute. It also maps the generated Access-Network-Charging- Identifier
11 Values to the WiMAX PDFIDs (Packet Data Flow Identifiers). It includes both the translated attributes, i.e. SDFID
12 and PDFIDs plus the Access-Network-Charging-Address (IP address of the CDR generator) in the accounting
13 records send to the OFCS via AAA. The AAA server will provide an attribute translation of the SDFID and PDFID
14 attributes to AF-Charging-Identifier and ANCID attributes before sending the accounting records to the OFCS.
15

- 1
- 2
- 3

Figure 20: End to end offline charging scenario

4

5
6
7
8
9
10

11

12
13
14
15

16
17
18
19

20

21

22

PCC

AAA Message	Triggering Events
Diameter ACR [Start] Radius Acct-Request [Start]	When a packet data flow is created upon: <ul style="list-style-type: none"> IP-CAN session establishment IP-CAN bearer establishment during IP-CAN session modification
	Upon Accounting client relocation (see note 1)
	At the onset or reset of Hot-Lining of an ongoing IP-CAN session (see note 2)
	Due to overflow of any of the counters (see note 2)
	At a specific time of the day (see note 2 and 3)
	Change of charging conditions. E.g., QoS change (see note 4)
Diameter ACR [Interim] Radius Acct-Request [Interim]	•
	By accounting interim interval (see note 5)
	Upon idle mode transition (see note 6)
Diameter ACR [Stop] Radius Acct-Request [Stop]	When a packet data flow is terminated upon: <ul style="list-style-type: none"> IP-CAN session termination IP-CAN bearer termination during IP-CAN session modification
	Upon Accounting client relocation (see note 1)
	At the onset or reset of Hot-Lining of an ongoing IP-CAN session (see note 2)
	Due to overflow of any of the counters (see note 2)
	At a specific time of the day (see note 2 and 3)
	Change of charging conditions. E.g., QoS change (see note 4)
NOTE 1: A new Accounting client generates an Accounting-Request Start with Beginning-of-Session AVP (=FALSE or Missing). An old Accounting client generates an Accounting-Request Stop with Session-Continue AVP (=TRUE).	
NOTE 2: Functions defined in NWG R1 to support accounting segmentation. The Accounting-Request Start includes Beginning-of-Session AVP (=FALSE or Missing) and the Accounting-Request Stop includes Session-Continue AVP (=TRUE), respectively.	
NOTE 3: Function defined in NWG R1 accounting, e.g. when the AAA delivers Time-Of-Day-Time AVP in the Access-Accept for the offline tariff change.	
NOTE 4: When a packet data flow is modified relevant to charging conditions (e.g., QoS changes), an accounting Stop message is generated followed by an accounting Start message to report the modified information so that it can be used for a charging purpose.	
NOTE 5: An accounting client may optionally generate periodic interim accounting messages according to its own configuration. However, if Accounting-Interim-Interval AVP is delivered from the AAA, interim accounting messages SHALL be generated and sent to the AAA periodically. The interim message includes Interim-Cause AVP set to INTERIM_INTERVAL(1).	
NOTE 6: Function defined in NWG R1 accounting. The anchor authenticator knows when an MS enters or exits the idle mode. The accounting client collocated at the anchor authenticator may notify the AAA at the CSN of the idle mode transition using the accounting messages. The ASN SHALL only send an idle mode notification against the ISF. The interim message includes Interim-Cause AVP set to IDLE_MODE_TRANSITION(2).	

- 1
- 2 **9.5.4 Overview of Diameter AVPs used for PCC-R3-OFC and PCC-R3-OFC' Reference**
- 3 **points**
- 4 If not differently mentioned, AVPs can be used in all kinds of WiMAX offline charging, including IP session based,
- 5 PD flow based, and PCC based charging. All AVPs which are referenced in this section are allowed to be used for
- 6 any kind of offline charging as far as there is no explicit restriction mentioned in this section or at the description of
- 7 the AVP.
- 8
- 9 Table 6 provides the list of IETF Reused AVPs.

1

Table 6: IETF Reused AVPs

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
Session-Id	263	UTF8String	RFC 3588	M	P	-	V	Y
Origin-Host	264	DiamIdentity	RFC 3588	M	P	-	V	N
Origin-Realm	296	DiamIdentity	RFC 3588	M	P	-	V	N
Destination-Realm	283	DiamIdentity	RFC 3588	M	P	-	V	N
Accounting-Record-Type	480	Enumerated	RFC 3588	M	P	-	V	Y
Accounting-Record-Number	485	Unsigned32	RFC 3588	M	P	-	V	Y
Acct-Application-Id	259	Unsigned32	RFC 3588	M	P	-	V	N
User-Name	1	UTF8String	RFC 3588	M	P	-	V	Y
Acct-Session-Id	44	OctetString	RFC 3588	M	P	-	V	Y
Acct-Multi-Session-Id	50	Unsigned32	RFC 3588	M	P	-	V	Y
Origin-State-Id	278	Unsigned32	RFC 3588	M	P	-	V	N
Destination-Host	293	DiamIdentity	RFC 3588	M	P	-	V	N
Event-Timestamp	55	Time	RFC 3588	M	P	-	V	N
Acct-Delay-Time	41	Unsigned32	RFC 4005	M	P	-	V	Y
NAS-Identifier	32	UTF8String	RFC 4005	M	P	-	V	Y
NAS-IP-Address	4	OctetString	RFC 4005	M	P	-	V	Y
NAS-IPv6-Address	95	OctetString	RFC 4005	M	P	-	V	Y
NAS-Port-Type	61	Enumerated	RFC 4005	M	P	-	V	Y
Class	25	OctetString	RFC 3588	M	P	-	V	Y
Termination-Cause	295	Enumerated	RFC 3588	M	P	-	V	Y
Accounting-Input-Octets	363	Unsigned64	RFC 4005	M	P	-	V	Y
Accounting-Input-Packets	365	Unsigned64	RFC 4005	M	P	-	V	Y
Accounting-Output-Octets	364	Unsigned64	RFC 4005	M	P	-	V	Y
Accounting-Output-Packets	366	Unsigned64	RFC 4005	M	P	-	V	Y
Acct-Link-Count	51	Unsigned32	RFC 4005	M	P	-	V	Y
Acct-Session-Time	46	Unsigned32	RFC 4005	M	P	-	V	Y
Calling-Station-Id	31	UTF8String	RFC 4005	M	P	-	V	Y
Accounting-Realtime-Required	483	Enumerated	RFC 3588	M	P	-	V	Y
Acct-Interim-Interval	85	Unsigned32	RFC 3588	M	P	-	V	Y
Framed-IP-Address	8	OctetString	RFC 4005	M	P	-	V	Y
Framed-Ipv6-Prefix	97	OctetString	RFC 4005	M	P	-	V	Y
Framed-Interface-Id	96	Unsigned64	RFC 4005	M	P	-	V	Y
Proxy-Info	284	Grouped	RFC 3588	M	-	-	P,V	N
Route-Record	282	DiamIdentity	RFC 3588	M	-	-	P,V	N
CUI	89	UTF8String	RFC 4372	M	P	-	V	Y
Result-Code	268	Unsigned32	RFC 3588	M	P	-	V	N
Error-Message	281	UTF8String	RFC 3588	-	P	-	V,M	N
Error-Reporting-Host	294	DiamIdentity	RFC 3588	-	P	-	V,M	N
Failed-AVP	279	Grouped	RFC 3588	M	P	-	V	N
Service-Context-Id	461	UTF8String	RFC 4006	M	P	-	V	Y

2

3 3GPP reused AVPs are listed in Table 7.

Table 7: 3GPP Reused AVPs

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
Service-Information	873	Grouped	TS 32.299	V,M	P	-	-	N
QoS-Class-Identifier	1028	Enumerated	TS 29.212	V,M	P	-	-	Y
Maximum-Requested-Bandwidth-UL	516	Unsigned32	TS 29.214	V,M	P	-	-	Y
Maximum-Requested-Bandwidth-DL	515	Unsigned32	TS 29.214	V,M	P	-	-	Y
Guaranteed-Bitrate-UL	1025	Unsigned32	TS 29.212	V,M	P	-	-	Y
Guaranteed-Bitrate-DL	1026	Unsigned32	TS 29.212	V,M	P	-	-	Y
Access-Network-Charging-Identifier-Value	503	OctetString	TS 29.214	V,M	P	-	-	Y
AF-Correlation-Information	1276	Grouped	TS 32.299	V,M	P	-	-	N
AF-Charging-Identifier	505	OctetString	TS 29.214	V,M	P	-	-	Y
Flows	510	Grouped	TS 29.214	V,M	P	-	-	Y
Media-Component-Number	518	Unsigned32	TS 29.214	V,M	P	-	-	Y
Flow-Number	509	Unsigned32	TS 29.214	V,M	P	-	-	Y
Charging-Information	618	Grouped	TS 29.229	V,M	-	-	-	N
Primary-Charging-Collection-Function-Name	621	DiameterURI	TS 29.229	V,M	-	-	-	N
Secondary-Charging-Collection-Function-Name	622	DiameterURI	TS 29.229	V,M	-	-	-	N
Access-Network-Charging-Address	501	Address	TS 29.214	V,M	P	-	-	Y

WiMAX specific AVPs are presented in Table 8.

Table 8: WiMAX Specific AVPs

AVP Name	AVP Code	Value Type	Reference	AVP Flag rules				
				Must	May	Should not	Must not	May Encr.
Session-Continue	21	Enumerated	[11]	V,M	P	-	-	N
Beginning-of-Session	22	Enumerated	[11]	V,M	P	-	-	N
IP-Technology	23	Enumerated	[11]	V,M	P	-	-	N
Hotline-Indicator	24	OctetString	[11]	V,M	P	-	-	N
Hotlining-Capabilities	303	Unsigned32	[11]	V,M	P	-	-	N
Prepaid-Indicator	25	Enumerated	[11]	V,M	P	-	-	N
Idle-Mode-Transition	44	Enumerated	[11]	V,M	P	-	-	N
Count-Type	59	Enumerated		V,M	P	-	-	N
SDFID	27	OctetString	9.7.2.3	V,M	P	-	-	N
PDFID	26	OctetString	9.7.2.4	V,M	P	-	-	N
hHA-IP-MIP4	6	Address	[11]	V,M	P	-	-	N
hHA-IP-MIP6	7	Address	[11]	V,M	P	-	-	N
NAP-ID	45	OctetString	[11]	V,M	P	-	-	N
NSP-ID	57	OctetString	[11]	V,M	P	-	-	N
BS-ID	46	OctetString	[11]	V,M	P	-	-	N
Location	47	OctetString	[11]	V,M	P	-	-	N
GMT-Time-Zone-Offset	3	Integer32	[11]	V,M	P	-	-	N
Active-Time	39	Unsigned64	[11]	V,M	P	-	-	N
Control-Packets-In	31	Unsigned64	[11]	V,M	P	-	-	N
Control-Packets-Out	33	Unsigned64	[11]	V,M	P	-	-	N
Control-Octets-In	32	Unsigned64	[11]	V,M	P	-	-	N
Control-Octets-Out	34	Unsigned64	[11]	V,M	P	-	-	N
Uplink-Flow-Description	50	IPFilterRule	9.7.2.5	V,M	P	-	-	N
Downlink-Flow-Description	62	IPFilterRule	9.7.2.6	V,M	P	-	-	N
Uplink-Granted-QoS	30	Grouped	9.7.2.7	V,M	P	-	-	N
Downlink-Granted-QoS	63	Grouped	9.7.2.8	V,M	P	-	-	N
QoS-ID	312	Unsigned32	[11]	V,M	P	-	-	N
Global-Service-Class-Name	313	UTF8String	[11]	V,M	P	-	-	N
Service-Class-Name	314	UTF8String	[11]	V,M	P	-	-	N
Schedule-Type	315	Enumerated	[11]	V,M	P	-	-	N
Traffic-Priority	316	Unsigned32	[11]	V,M	P	-	-	N
Maximum-Sustained-Traffic-Rate	317	Unsigned32	[11]	V,M	P	-	-	N
Minimum-Reserved-Traffic-Rate	318	Unsigned32	[11]	V,M	P	-	-	N
Maximum-Traffic-Burst	319	Unsigned32	[11]	V,M	P	-	-	N
Tolerated-Jitter	320	Unsigned32	[11]	V,M	P	-	-	N
Maximum-Latency	321	Unsigned32	[11]	V,M	P	-	-	N
Reduced-Resources-Code	322	Enumerated	[11]	V,M	P	-	-	N
Media-Flow-Type	323	Enumerated	[11]	V,M	P	-	-	N
Unsolicited-Grant-Interval	325	Unsigned32	[11]	V,M	P	-	-	N
SDU-Size	326	Unsigned32	[11]	V,M	P	-	-	N
Unsolicited-Polling-Interval	327	Unsigned32	[11]	V,M	P	-	-	N
Media-Flow-Description-In-SDP-Format	324	OctetString	[11]	V,M	P	-	-	N
Transmission-Policy	412	OctetString		V,M	P	-	-	N
Trigger	1264	Grouped	[9]	V,M	P	-	-	N
Trigger-Type	870	Enumerated	[9]	V,M	P	-	-	N
Unit-Quota-Threshold	1226	Unsigned32	[9]	V,M	P	-	-	N
Visited-Framed-IP-Address	79	OctetString	[11]	V,M	P	-	-	N
Visited-Framed-Ipv6-Prefix	80	OctetString	[11]	V,M	P	-	-	N
Visited-Framed-Interface-Id	81	Unsigned64	[11]	V,M	P	-	-	N
Volume-Quota-Threshold	869	Unsigned32	[9]	V,M	P	-	-	N
Direction	306	Enumerated	9.7.2.9	V,M	P	-	-	N
Interim-Cause	413	Enumerated	[11]	V,M	P	-	-	N
WiMAX-Information	409	Grouped	9.7.1.2	V,M	P	-	-	N
WiMAX-QoS-Information	407	Grouped	9.4.2.2.1	V,M	P	-	-	Y

1
2

PCC

9.5.5 Accounting Messages over PCC-R3-OFC Reference Point**9.5.5.1 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 ]
    * [ Class ]
    [ Termination-Cause ]
    [ Accounting-Input-Octets ]
    [ Accounting-Input-Packets ]
    [ Accounting-Output-Octets ]
    [ Accounting-Output-Packets ]
    [ Acct-Link-Count ]
    [ Acct-Session-Time ]
    [ Calling-Station-Id ]
    [ Accounting-Realtime-Required ]
    [ Acct-Interim-Interval ]
    [ Framed-IP-Address ]
    [ Framed-IPv6-Prefix ]
    [ Framed-Interface-Id ]
    [ CUI ]
    * [ Proxy-Info ]
    * [ Route-Record ]

    [ Session-Continue ]
    [ Beginning-Of-Session ]
    [ IP-Technology ]
    [ Hotline-Indicator ]
    [ Prepaid-Indicator ]
    [ Idle-Mode-Transition ]
    [ Count-Type ]
    [ SDFID ]
    [ PDFID ]
    [ hHA-IP-MIP4 ]
    [ hHA-IP-MIP6 ]
    [ NAP-ID ]
    [ NSP-ID ]
    [ BS-ID ]
    [ Location ]
    [ GMT-Time-Zone-Offset ]
    [ Active-Time ]

```

PCC

```

1          [ Control-Packets-In ]
2          [ Control-Packets-Out ]
3          [ Control-Octets-In ]
4          [ Control-Octets-Out ]
5      * [ Uplink-Flow-Description ]
6      * [ Downlink-Flow-Description ]
7          [ Uplink-Granted-Qos ]
8          [ Downlink-Granted-Qos ]
9          [ Visited-Framed-IP-Address ]
10         [ Visited-Framed-Ipv6-Prefix ]
11         [ Visited-Framed-Interface-Id ]
12         [ Direction ]
13         [ Interim-Cause ]
14
15         [ WiMAX-QoS-Information ]
16         [ AF-Correlation-Information ]
17         [ Charging-Information ]
18     * [ AVP ]
19

```

20 9.5.5.2 Accounting-Answer Message

21 Diameter Accounting-Answer message over the PCC-R3-OFC is defined as follows:

22 It can be used for the IP session based or PD flow based charging as well as for the PCC based charging.

```

23
24 <AC-Answer> ::= < Diameter Header: 271, PXY >
25     < Session-Id >
26     { Result-Code }
27     { Origin-Host }
28     { Origin-Realm }
29     { Accounting-Record-Type }
30     { Accounting-Record-Number }
31     [ Acct-Application-Id ]
32     [ User-Name ]
33     [ Acct-Session-Id ]
34     [ Acct-Multi-Session-Id ]
35     [ Event-Timestamp ]
36     [ Error-Message ]
37     [ Error-Reporting-Host ]
38     * [ Failed-AVP ]
39     [ Origin-State-Id ]
40     [ Termination-Cause ]
41     [ Accounting-Realtime-Required ]
42     [ Acct-Interim-Interval ]
43     * [ Class ]
44     * [ Proxy-Info ]
45     * [ Route-Record ]
46     * [ AVP ]
47
48
49

```

50 9.5.6 AVP Occurrence Table

51 Table 9 shows which AVPs are to be present and used in accounting messages between the accounting client and the
52 AAA, according to each accounting mode.

Table 9: AVP Occurrence Table

AVP Name	Accounting mode			Accounting-Request			Accounting-Answer		
	Non-PCC		PCC	START	INTERIM	STOP	START	INTERIM	STOP
	IP	PD flow							
Session-Id	X	X	X	1	1	1	1	1	1
Origin-Host	X	X	X	1	1	1	1	1	1
Origin-Realm	X	X	X	1	1	1	1	1	1
Destination-Realm	X	X	X	1	1	1	0	0	0
Accounting-Record-Type	X	X	X	1	1	1	1	1	1
Accounting-Record-Number	X	X	X	1	1	1	1	1	1
Acct-Application-Id	X	X	X	1	1	1	1	1	1
User-Name	X	X	X	1	1	1	1	1	1
Acct-Session-Id	X	X	X	1	1	1	1	1	1
Acct-Multi-Session-Id	X	X	X	1	1	1	1	1	1
Origin-State-Id	X	X	X	0-1	0-1	0-1	0-1	0-1	0-1
Destination-Host	X	X	X	0-1	0-1	0-1	0	0	0
Event-Timestamp	X	X	X	1	1	1	0-1	0-1	0-1
Acct-Delay-Time	X	X	X	0-1	0-1	0-1	0	0	0
NAS-Identifier	X	X	X	0-1	0-1	0-1	0	0	0
NAS-IP-Address	X	X	X	0-1[1]	0-1[1]	0-1[1]	0	0	0
NAS-IPv6-Address	X	X	X	0-1[1]	0-1[1]	0-1[1]	0	0	0
NAS-Port-Type	X	X	X	0-1	0-1	0-1	0	0	0
Class	X	X	X	0+ [2]	0+ [2]	0+ [2]	0+	0+	0+
Termination-Cause	X	X	X	0	0	1	0	0	0-1
Accounting-Input-Octets	X	X	X	0	1	1	0	0	0
Accounting-Input-Packets	X	X	X	0	1	1	0	0	0
Accounting-Output-Octets	X	X	X	0	1	1	0	0	0
Accounting-Output-Packets	X	X	X	0	1	1	0	0	0
Acct-Link-Count	X	X	X	0-1	0-1	0-1	0	0	0
Acct-Session-Time	X	X	X	0	0-1	0-1	0	0	0
Calling-Station-Id	X	X	X	0-1	0-1	0-1	0	0	0
Accounting-Realtime-Required	X	X	X	0-1	0-1	0-1	0-1	0-1	0-1
Acct-Interim-Interval	X	X	X	0-1	0-1	0-1	0-1	0-1	0-1
Framed-IP-Address	X	X	X	0-1[3]	0-1[3]	0-1[3]	0	0	0
Framed-Ipv6-Prefix	X	X	X	0-1[3]	0-1[3]	0-1[3]	0	0	0
Framed-Interface-Id	X	X	X	0-1[3]	0-1[3]	0-1[3]	0	0	0
Visited-Framed-IP-Address	X	X	X	0-1	0-1	0-1	0	0	0
Visited-Framed-Ipv6-Prefix	X	X	X	0-1	0-1	0-1	0	0	0
Visited-Framed-Interface-Id	X	X	X	0-1	0-1	0-1	0	0	0
Proxy-Info	X	X	X	0+	0+	0+	0+	0+	0+
Route-Record	X	X	X	0+	0+	0+	0+	0+	0+
CUI	X	X	X	0-1[4]	0-1[4]	0-1[4]	0	0	0
Result-Code	X	X	X	0	0	0	1	1	1
Error-Message	X	X	X	0	0	0	0-1	0-1	0-1
Error-Reporting-Host	X	X	X	0	0	0	0-1	0-1	0-1
Failed-AVP	X	X	X	0	0	0	0-1	0-1	0-1
Session-Continue	X	X	X	0	0	0-1[5]	0	0	0
Beginning-of-Session	X	X	X	0-1[5]	0	0	0	0	0
IP-Technology	X	X	X	0-1[5]	0-1[5]	0-1[5]	0	0	0
Hotline-Indicator	X	X	X	0-1[6]	0-1[6]	0-1[6]	0	0	0
Prepaid-Indicator	X	X	X	0-1	0-1	0-1	0	0	0
Idle-Mode-Transition	X	X	X	0	0-1[7]	0	0	0	0
Count-Type	X	X	X	0	0-1[8]	0-1[8]	0	0	0
hHA-IP-MIP4	X	X	X	0-1	0-1	0-1	0	0	0
hHA-IP-MIP6	X	X	X	0-1	0-1	0-1	0	0	0
NAP-ID	X	X	X	0-1[9]	0-1[9]	0-1[9]	0	0	0
BS-ID	X	X	X	0-1[9]	0-1[9]	0-1[9]	0	0	0
NSP-ID	X	X	X	0-1[10]	0-1[10]	0-1[10]	0	0	0
Location	X	X	X	0-1	0-1	0-1	0	0	0

PCC

AVP Name	Accounting mode			Accounting-Request			Accounting-Answer		
	Non-PCC		PCC	START	INTERIM	STOP	START	INTERIM	STOP
	IP	PD flow							
GMT-Time-Zone-Offset	X	X	X	0-1	0-1	0-1	0	0	0
Active-Time	X	X	X	0	0-1[11]	0-1[11]	0	0	0
Control-Packets-In	X	X	X	0	0-1[11]	0-1[11]	0	0	0
Control-Packets-Out	X	X	X	0	0-1[11]	0-1[11]	0	0	0
Control-Octets-In	X	X	X	0	0-1[11]	0-1[11]	0	0	0
Control-Octets-Out	X	X	X	0	0-1[11]	0-1[11]	0	0	0
Interim-Cause	X	X	X	0	1	0	0	0	0
SDFID	-	X	X	0-1[12]	0-1[12]	0-1[12]	0	0	0
PDFID	-	X	X	0-1[13]	0-1[13]	0-1[13]	0	0	0
Uplink-Flow-Description	-	X	X	0	0+[14]	0+[14]	0	0	0
Downlink-Flow-Description	-	X	X	0	0+[14]	0+[14]	0	0	0
Uplink-Granted-QoS	-	X	X	0-1	0-1[15]	0-1[15]	0	0	0
Downlink-Granted-QoS	-	X	X	0-1	0-1[15]	0-1[15]	0	0	0
QoS-ID	-	X	X	0-1	0-1	0-1	0	0	0
Global-Service-Class-Name	-	X	X	0-1	0-1	0-1	0	0	0
Service-Class-Name	-	X	X	0-1	0-1	0-1	0	0	0
Schedule-Type	-	X	X	0-1	0-1	0-1	0	0	0
Traffic-Priority	-	X	X	0-1	0-1	0-1	0	0	0
Maximum-Sustained-Traffic-Rate	-	X	X	0-1	0-1	0-1	0	0	0
Minimum-Reserved-Traffic-Rate	-	X	X	0-1	0-1	0-1	0	0	0
Maximum-Traffic-Burst	-	X	X	0-1	0-1	0-1	0	0	0
Tolerated-Jitter	-	X	X	0-1	0-1	0-1	0	0	0
Maximum-Latency	-	X	X	0-1	0-1	0-1	0	0	0
Reduced-Resources-Code	-	X	X	0-1	0-1	0-1	0	0	0
Media-Flow-Type	-	X	X	0-1	0-1	0-1	0	0	0
Unsolicited-Grant Interval	-	X	X	0-1	0-1	0-1	0	0	0
SDU-Size	-	X	X	0-1	0-1	0-1	0	0	0
Unsolicited-Polling-Interval	-	X	X	0-1	0-1	0-1	0	0	0
Media-Flow-Description-In-SDP-Format	-	X	X	0-1	0-1	0-1	0	0	0
Transmission-Policy	-	X	X	0-1	0-1	0-1	0	0	0
Direction	-	X	X	0-1	0-1	0-1	0	0	0
WiMAX-QoS-Information	-	-	X	0-1	0-1	0-1	0	0	0
QoS-Class-Identifier	-	-	X	0-1	0-1	0-1	0	0	0
Maximum-Requested-Bandwidth-UL	-	-	X	0-1	0-1	0-1	0	0	0
Maximum-Requested-Bandwidth-DL	-	-	X	0-1	0-1	0-1	0	0	0
Guaranteed-Bitrate-UL	-	-	X	0-1	0-1	0-1	0	0	0
Guaranteed-Bitrate-DL	-	-	X	0-1	0-1	0-1	0	0	0
Bearer-Identifier	-	-	X	0-1	0-1	0-1	0	0	0
AF-Correlation-Information	-	-	X	0-1	0-1	0-1	0	0	0
AF-Charging-Identifier	-	-	X	0-1	0-1	0-1	0	0	0
Flows	-	-	X	0-1	0-1	0-1	0	0	0
Media-Component-Number	-	-	X	0-1	0-1	0-1	0	0	0
Flow-Number	-	-	X	0-1	0-1	0-1	0	0	0
Charging-Information	-	-	X	0-1	0-1	0-1	0	0	0
Primary-Charging-Collection-Function-Name	-	-	X	0-1	0-1	0-1	0	0	0
Secondary-Charging-Collection-Function-Name	-	-	X	0-1	0-1	0-1	0	0	0

1

2 **Notes:**

- [1] At least one of NAS-IP-Address or NAS-IPv6-Address SHALL appear in the Accounting message.
- [2] Class SHALL be included if received in the Diameter DEA command.

PCC

- [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 hotlined, 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.

9.5.7 Accounting Messages over PCC-R3-OFC' Reference Point

9.5.7.1 Accounting-Request Message

Diameter Accounting-Request message used in the PCC-R3-OFC' reference point is defined according to Rf reference point [9]. The message format is defined as follows:

```

<AC-Request> ::= < Diameter Header: 271, REQ, PXY >
                < Session-Id >
                { Origin-Host }
                { Origin-Realm }
                { Destination-Realm }
                { Accounting-Record-Type }
                { Accounting-Record-Number }
  
```

PCC

```

1          [ Acct-Application-Id ]
2          [ User-Name ]
3          [ Acct-Interim-Interval ]
4          [ Origin-State-Id ]
5          [ Event-Timestamp ]
6          * [ Proxy-Info ]
7          * [ Route-Record ]
8          [ Service-Context-Id ]
9          [ Service-Information ]
10         * [ AVP ]
11

```

9.5.7.2 Accounting-Answer Message

Diameter Accounting-Answer message used in the PCC-R3-OFC' reference point is based on the Rf reference point [9]. The message format is defined as follows:

```

15
16 <AC-Answer> ::= < Diameter Header: 271, PXY >
17                < Session-Id >
18                { Result-Code }
19                { Origin-Host }
20                { Origin-Realm }
21                { Accounting-Record-Type }
22                { Accounting-Record-Number }
23                [ Acct-Application-Id ]
24                [ User-Name ]
25                [ Acct-Session-Id ]
26                [ Acct-Multi-Session-Id ]
27                [ Error-Reporting-Host ]
28                [ Acct-Interim-Interval ]
29                [ Origin-State-Id ]
30                [ Event-Timestamp ]
31                * [ Proxy-Info ]
32                * [ AVP ]

```

9.5.8 AVP Occurrence Table

Table 10 shows which AVPs are to be present and used between the AAA and the OFCS, for the PCC based charging.

Table 10: AVP Occurrence Table

AVP Name	Accounting-Request			Accounting-Answer		
	START	INTERIM	STOP	START	INTERIM	STOP
Session-Id	1	1	1	1	1	1
Origin-Host	1	1	1	1	1	1
Origin-Realm	1	1	1	1	1	1
Destination-Realm	1	1	1	0	0	0
Accounting-Record-Type	1	1	1	1	1	1
Accounting-Record-Number	1	1	1	1	1	1
Acct-Application-Id	1	1	1	1	1	1
User-Name	1	1	1	1	1	1
Acct-Session-Id	1	1	1	1	1	1
Acct-Multi-Session-Id	1	1	1	1	1	1
Origin-State-Id	0-1	0-1	0-1	0-1	0-1	0-1
Destination-Host	0-1	0-1	0-1	0	0	0
Event-Timestamp	1	1	1	0-1	0-1	0-1
Acct-Delay-Time	0-1	0-1	0-1	0	0	0
NAS-Identifier	0-1	0-1	0-1	0	0	0
NAS-Port-Type	0-1	0-1	0-1	0	0	0
Class	0+	0+	0+	0+	0+	0+
Termination-Cause	0	0	1	0	0	0-1
Accounting-Input-Octets	0	0-1	0-1	0	0	0
Accounting-Input-Packets	0	0-1	0-1	0	0	0
Accounting-Output-Octets	0	0-1	0-1	0	0	0
Accounting-Output-Packets	0	0-1	0-1	0	0	0
Acct-Link-Count	0-1	0-1	0-1	0	0	0
Acct-Session-Time	0	0-1	0-1	0	0	0
Calling-Station-Id	0-1	0-1	0-1	0	0	0
Accounting-Realtime-Required	0-1	0-1	0-1	0-1	0-1	0-1
Acct-Interim-Interval	0-1	0-1	0-1	0-1	0-1	0-1
Framed-IP-Address	0-1	0-1	0-1	0	0	0
Framed-Ipv6-Prefix	0-1	0-1	0-1	0	0	0
Framed-Interface-Id	0-1	0-1	0-1	0	0	0
Proxy-Info	0+	0+	0+	0+	0+	0+
Route-Record	0+	0+	0+	0+	0+	0+
CUI	0-1	0-1	0-1	0	0	0
Result-Code	0	0	0	1	1	1
Error-Message	0	0	0	0-1	0-1	0-1
Error-Reporting-Host	0	0	0	0-1	0-1	0-1
Failed-AVP	0	0	0	0-1	0-1	0-1
Session-Continue	0	0	0-1	0	0	0
Beginning-of-Session	0-1	0	0	0	0	0
IP-Technology	0-1	0-1	0-1	0	0	0
Hotline-Indicator	0-1	0-1	0-1	0	0	0
Prepaid-Indicator	0-1	0-1	0-1	0	0	0
Idle-Mode-Transition	0	0-1	0	0	0	0
Count-Type	0	0-1	0-1	0	0	0
hHA-IP-MIP4	0-1	0-1	0-1	0	0	0
hHA-IP-MIP6	0-1	0-1	0-1	0	0	0
NAP-ID	0-1	0-1	0-1	0	0	0
NSP-ID	0-1	0-1	0-1	0	0	0
BS-ID	0-1	0-1	0-1	0	0	0
Location	0-1	0-1	0-1	0	0	0
GMT-Time-Zone-Offset	0-1	0-1	0-1	0	0	0
Active-Time	0	0-1	0-1	0	0	0
Control-Packets-In	0	0-1	0-1	0	0	0
Control-Packets-Out	0	0-1	0-1	0	0	0
Control-Octets-In	0	0-1	0-1	0	0	0
Control-Octets-Out	0	0-1	0-1	0	0	0

PCC

AVP Name	Accounting-Request			Accounting-Answer		
	START	INTERIM	STOP	START	INTERIM	STOP
Uplink-Flow-Description	0	0-n	0-n	0	0	0
Downlink-Flow-Description	0	0-n	0-n	0	0	0
Uplink-Granted-QoS	0	0-1	0-1	0	0	0
Downlink-Granted-QoS	0	0-1	0-1	0	0	0
QoS-ID	0	0-1	0-1	0	0	0
Global-Service-Class-Name	0	0-1	0-1	0	0	0
Service-Class-Name	0	0-1	0-1	0	0	0
Schedule-Type	0	0-1	0-1	0	0	0
Traffic-Priority	0	0-1	0-1	0	0	0
Maximum-Sustained-Traffic-Rate	0	0-1	0-1	0	0	0
Minimum-Reserved-Traffic-Rate	0	0-1	0-1	0	0	0
Maximum-Traffic-Burst	0	0-1	0-1	0	0	0
Tolerated-Jitter	0	0-1	0-1	0	0	0
Maximum-Latency	0	0-1	0-1	0	0	0
Reduced-Resources-Code	0	0-1	0-1	0	0	0
Media-Flow-Type	0	0-1	0-1	0	0	0
Unsolicited-Grant Interval	0	0-1	0-1	0	0	0
SDU-Size	0	0-1	0-1	0	0	0
Unsolicited-Polling-Interval	0	0-1	0-1	0	0	0
Media-Flow-Description-In-SDP-Format	0	0-1	0-1	0	0	0
Transmission-Policy	0	0-1	0-1	0	0	0
Visited-Framed-IP-Address	0-1	0-1	0-1	0	0	0
Visited-Framed-Ipv6-Prefix	0-1	0-1	0-1	0	0	0
Visited-Framed-Interface-Id	0-1	0-1	0-1	0	0	0
Direction	0	0-1	0-1	0	0	0
Interim-Cause	0	1	0	0	0	0
Service-Context-Id	0-1	0-1	0-1	0	0	0
Service-Information	1	1	1	0	0	0
WiMAX-Information	1	1	1	0	0	0
WiMAX-QoS-Information	0-1	0-1	0-1	0	0	0
QoS-Class-Identifier	0-1	0-1	0-1	0	0	0
Maximum-Requested-Bandwidth-UL	0-1	0-1	0-1	0	0	0
Maximum-Requested-Bandwidth-DL	0-1	0-1	0-1	0	0	0
Guaranteed-Bitrate-UL	0-1	0-1	0-1	0	0	0
Guaranteed-Bitrate-DL	0-1	0-1	0-1	0	0	0
Bearer-Identifier	0-1	0-1	0-1	0	0	0
Access-Network-Charging-Identifier-Value	0-1	0-1	0-1	0	0	0
AF-Correlation-Information	0-1	0-1	0-1	0	0	0
AF-Charging-Identifier	0-1	0-1	0-1	0	0	0
Flows	0-1	0-1	0-1	0	0	0
Media-Component-Number	0-1	0-1	0-1	0	0	0
Flow-Number	0-1	0-1	0-1	0	0	0
Charging-Information	0-1	0-1	0-1	0	0	0
Primary-Charging-Collection-Function-Name	0-1	0-1	0-1	0	0	0
Secondary-Charging-Collection-Function-Name	0-1	0-1	0-1	0	0	0
Access-Network-Charging-Address	0-1	0-1	0-1	0	0	0

- 1
- 2 **9.6 Diameter based Online Charging**
- 3 Diameter based Online Charging is based on the definition specified in [11]. The PCC-R3-OC interface is defined
- 4 between Anchor SFA and Online Charging System (OCS)/Pre-Paid Server (PPS) and correspond to the R3-OC
- 5 specified in [11] with PCC specific extension.

PCC

The PCC-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.

For PCC support, 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.

9.6.1 PCC-R3-OC Interface Definition

The PCC-R3-OC protocol is based on R3-OC [11] and the Diameter Credit Control [RFC4006] protocol with additional optional AVPs.

With regard to the Diameter protocol defined over the PCC-R3-OC interface, PPS acts as a Diameter online charging server, i.e., it is the network element that handles Credit Control Requests for a particular MS. The PPC acts as the Diameter online charging client, i.e., it is the network element requesting credits from PPS, and returns the consumption information about the consumed credits to PPS.

For existing AVPs predefined vendor codes are used. For AVPs introduced by WiMAX, the WiMAX vendor ID SHALL be used.

9.6.1.1 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 [18].

After establishing the transport connection, the PPC and the PPS shall advertise the support of the PCC-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 [18]).

The termination of the Diameter user session is specified in RFC 3588 [18]. The description of how to use these termination procedures in the normal cases is embedded in the procedures description.

9.6.1.1.1 PCC-R3-OC Auth-Application-ID

A new vendor specific Diameter Auth-Application-ID is defined for WiMAX.

The PCC-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 [18]) under Applications IDs.

9.6.1.2 PCC-R3-OC specific AVPs

PCC-R3-OC is based on RFC4006 [16]. It uses a part of RFC4006 AVPs (base Diameter and Diameter applications), that are identified for All Access Types. PCC-R3-OC additionally uses the optional PCC-R3-OC specific AVPs defined here and listed in Table 11.

Table 11: PCC-R3-OC specific AVPs

Attribute Name	AVP Code	Reference	Value Type (note 2)	AVP Flag rules (note 1)				May Encr.
				Must	May	Should not	Must not	
R3-OC-Session-Continue	416	[11]	Enumerated	M,V	P			Y
Old-Session-Id	406	[11]	Integer32	M,V	P			Y
Service-Information	873	9.7.1.1	Grouped	M,V	P			Y
WiMAX-Information	409	[11]	Grouped	M,V	P			Y
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 [18].								
NOTE 2: The value types are defined in RFC 3588 [18].								

9.6.1.3 PCC-R3-OC Re-Used AVPs of external organizations

Table 12 lists the Diameter AVPs re-used by PCC-R3-OC interface from RFC4006 [16] and TS32.299 [9]. The other reused AVPs from the Diameter base protocol are not listed in Table 12.

Table 12 : PCC-R3-OC re-used Diameter AVPs

AVP	Reference	Description	Msg. Type
Access-Network-Charging-Identifier-Gx	9.4.2.3.1.5	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
AF-Charging-Identifier	[5]	This field contains the AF Charging Identifier that is sent by the AF.	CCR
AF-Correlation-Information	[9]	This field contains the "AF Charging Identifier" (ICID for IMS) and associated flow identifiers generated by the AF and received over PCC-R3-P/Gx and Rx.	CCR
Auth-Application-Id	[18]	This field identifies the Diameter Online application.	Both
CC-Input-Octets	[16]	This field contains the requested amount of octets to be received.	Both
CC-Output-Octets	[16]	This field contains the requested amount of octets to be sent.	Both
CC-Request-Type	[16]	This field defines the transfer type: event for event based charging and initial, update, terminate for session based charging.	Both
CC-Request-Number	[16]	This field contains the sequence number of the transferred messages.	Both
CC-Session-Failover	[16]	This field indicates if failover is supported.	CCA
CC-Service-Specific-Units	[16]	This field contains the requested amount of service specific units, e.g. number of events.	Both
CC-Time	[16]	This field contains the amount of requested time.	Both
CC-Total-Octets	[16]	This field contains the requested amount of octets to be sent and received.	Both
CC-Unit-Type	[16]	This field contains the type of units considered to be pooled.	CCA
Check-Balance-Result	[16]	This field contains the balance checking result.	CCA
Credit-Control-Failure-Handling	[16]	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	[16]	This field contains the cost information of a service, which the credit-control client can transfer transparently to the end user.	CCA
Cost-Unit	[16]	This field contains the unit of the Cost-Information as human readable string.	CCA
Currency-Code	[16]	This field identifies the currency.	CCA
Destination-Host	[18]	This field contains the destination peer address of the OCS identity.	CCR
Direct-Debiting-Failure-Handling	[16]	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	[18]	This field corresponds to the exact time the quota is requested	CCR
Exponent	[16]	This field contains the exponent value to be applied to Value-Digit-AVP.	CCA
Filter-Id	[15]	This field contains the name of the filter list for this user.	CCA
Final-Unit-Action	[16]	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	[16]	This field indicates that the Granted-Service-Unit containing the final units for the service.	CCA
Framed-IP-Address	[16]	The IPv4 address allocated for the user	Both

Framed-IPv6-Prefix	[16]	The IPv6 address prefix allocated for the user. The encoding of the value within this Octet String type AVP shall be as defined in IETF RFC 3162 [15], Clause 2.3. The "Reserved", "Prefix-Length" and "Prefix" fields shall be included in this order.	Both
Granted-Service-Unit	[16]	This field contains the amount of granted service units for a particular category.	CCA
G-S-U-Pool-Identifier	[9]	This field identifies a credit pool within the session.	CCA
G-S-U-Pool-Reference	[16]	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	9.7.3.1	This field contains all parameters for the CTF quota management and defines the quotas to allow traffic to flow.	Both
Multiple-Services-Indicator	[16]	This field indicates whether the CTF is capable of handling multiple services independently.	Both
Offline-Charging	[9]	This field contains a reference to the Offline Charging.	CCR
Origin-Host	[18]	This field identifies the endpoint of the originated Diameter message.	Both
Origin-Realm	[18]	This field contains the Realm of the originator of any Diameter message.	Both
Origin-State-Id	[18]		CCR
Proxy-Host	[18]	This field contains the identity of the host that added the Proxy-Info.	Both
Proxy-Info	[18]		Both
Proxy-State	[18]	This field contains local state information.	Both
Quota-Consumption-Time	[9]	This field contains an idle traffic threshold time in seconds.	CCA
Quota-Holding-Time	[9]	This field contains the quota holding time in seconds.	CCA
Rating-Group	[16]	This field contains the identifier of a rating group.	Both
Redirect-Address-Type	[16]	This field defines the address type of the address given in the Redirect-Server-Address field.	CCA
Redirect-Host	[18]	This field identifies the host where the message should be forwarded to.	CCA
Redirect-Host-Usage	[18]	This field dictates how the routing entry resulting from the Redirect-Host is to be used.	CCA
Redirect-Max-Cache-Time	[18]	This field contains the maximum number of seconds the peer and route table entries.	CCA
Redirect-Server	[16]	This field contains the address information of the redirect server.	CCA
Redirect-Server-Address	[16]	This field defines the address of the redirect server.	CCA
Remaining-Balance		This field contains the remaining balance of the subscriber.	CCA
Reporting-Reason	[9]	This field specifies the reason for usage reporting for one or more types of quota for a particular category.	CCR
Requested-Action	[16]	The field defines the type of action if the CC-Request-Type indicates EVENT.	CCR
Requested-Service-Unit	[16]	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 [16].	CCR
Restriction-Filter-Rule	[16]	This field provides filter rules corresponding to services that are to remain accessible.	CCA
Result-Code	[16]	This field contains the result of the query.	CCA
Route-Record	[18]		Both
Service-Context-Id	[16]	This field contains a unique identifier of the Diameter credit-control service specific document that applies to the request.	CCR

Service-Identifier	[16]	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	[18]	This field is used to identify a specific session.	Both
Subscription-Id	[16]	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	[16]	This field contains the user data content e.g. NAI for WiMAX.	CCR
Subscription-Id-Type	[16]	This field determines the type of the identifier, e.g. END_USER_NAI for WiMAX.	CCR
Tariff-Change-Usage	[16]	This field identifies the reporting period for the used service unit, i.e. before, after or during tariff change.	Both
Tariff-Time-Change	[16]	This field identifies the reporting period for the granted service units, i.e. before, after or during tariff change.	CCA
Termination-Cause	[18]	This field indicate the reason why a session was terminated.	CCR
Time-Quota-Mechanism	[9]		CCR
Time-Quota-Threshold	[9]	This field contains a threshold value in seconds.	CCA
Time-Quota-Type	[9]	This field indicate which time quota consumption mechanism shall be used for the associated Rating Group.	Both
Trigger	[9]	This field contains Trigger-Type.	Both
Trigger-Type	[9]	This field is used to negotiate triggers and when associated quota need to be re-authorised.	Both
Unit-Quota-Threshold	[9]	This field contains a threshold value in service specific units.	CCA
Unit-Value	[16]	This field specifies the units as decimal value.	CCA
User-Equipment-Info	[16]	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	[16]	This field determines the type of the identifier.	CCR
User-Equipment-Info-Value	[16]	This field contains the user MAC.	CCR
User-Name	[18]	This field contains the User-Name, in a format consistent with the NAI specification.	CCR
Used-Service-Unit	[16]	This field contains the amount of used non-monetary service units measured for a particular category to a particular quota type.	CCR
Value-Digits	[16]	This field contains the significant digits of the number.	CCA
Validity-Time	[16]	This field defines the time in order to limit the validity of the granted quota for a given category instance.	CCA
Volume-Quota-Threshold	[9]	This field contains a threshold value in octets.	CCA

9.6.1.4 PCC-R3-OC Messages

The following is the basic structure shared by all online charging messages. This is based directly on the format of the messages defined in IETF RFC 4006 [16] and modified in TS32.299 [9] and WiMAX Forum, T33-001-R015v01 “Detailed Protocols and Procedures, Base Specification”, Release 1.5 [11]. 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.

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.

PCC

1 Message format:

2 <CCR> ::= < Diameter Header: 272, REQ, PXY >

3
4 < Session-Id >

5 { Origin-Host }

6 { Origin-Realm }

7 { Destination-Realm }

8 { Auth-Application-Id }

9 { Service-Context-Id }

10 { CC-Request-Type }

11 { CC-Request-Number }

12 [Destination-Host]

13 [User-Name]

14 ~~[CC-Sub-Session-Id]~~

15 ~~[Acct-Multi-Session-Id]~~

16 [Origin-State-Id]

17 [Event-Timestamp]

18 *[Subscription-Id]

19 ~~[Service-Identifier]~~

20 [Termination-Cause]

21 ~~[Requested-Service-Unit]~~

22 [Requested-Action]

23 ~~[Used-Service-Unit]~~

24 [Multiple-Services-Indicator]

25 *[Multiple-Services-Credit-Control]

26 ~~[Service-Parameter-Info]~~

27 ~~[CC-Correlation-Id]~~

28 [User-Equipment-Info]

29 *[Proxy-Info]

30 *[Route-Record]

31 [Service-Information]

32 *[AVP]

34 Table 13 illustrates the basic structure of Diameter Credit Control Credit-Control-Request message as used for
35 Online Charging.

Table 13: 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	-	

PCC

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.

PCC

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 [9].
Trigger-Type	O _c	Used as defined in [9].
AF-Correlation-Information	O _c	This field contains the "AF Charging Identifier" (ICID for IMS) and associated flow identifiers generated by the AF and received over Rx/Gx. It is used in PCC scenario.
AVP	O _c	
Service-Parameter-Info	-	Not used in WiMAX.
Service-Parameter-Type	-	

PCC

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	
Offline-Charging	O _C	
AVP	O _C	

Note: See TS32.240-720 [7] for the meaning of "OM" and "OC".

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 }

```

PCC

```

1          [ Check-Balance-Result ]
2          [ Credit-Control-Failure-Handling ]
3          [ Direct-Debiting-Failure-Handling ]
4          { Validity-time }
5          * [ Redirect-Host ]
6          [ Redirect-Host-Usage ]
7          [ Redirect-Max-Cache-Time ]
8          * [ Proxy-Info ]
9          * [ Route-Record ]
10         * [ Failed-AVP ]
11         [ Service-Information ]
12         * [ AVP ]

```

Table 14 illustrates the basic structure of a Diameter Credit-Control-Answer message as used for online charging.

1

Table 14: 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.
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.

AVP	Category	Description
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.
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 an 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 [RFC4006].
Value-Digits	M	Used as defined in [RFC4006].
Exponent	O _c	Used as defined in [RFC4006].
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

AVP	Category	Description
		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 [9].
Unit-Quota-Threshold	O _c	Used as defined in [9].
Quota-Holding-Time	O _c	
Quota-Consumption-Time	O _c	
Trigger	O _c	Used as defined in [9].
Trigger-Type	O _c	Used as defined in [9].
AF-Correlation-Information	-	Not used in CCA.
AVP	-	
Cost-Information	O _c	Used as defined in [RFC4006].
Unit-Value	M	Used as defined in [RFC4006].
Value-Digits	M	Used as defined in [RFC4006].
Exponent	O _c	Used as defined in [RFC4006].
Currency-Code	M	Used as defined in [RFC4006].
Cost-Unit	O _c	Used as defined in [RFC4006].
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.
Unit-Value	M	Used as defined in [RFC4006].
Value-Digits	M	Used as defined in [RFC4006].
Exponent	O _c	Used as defined in [RFC4006].
Currency-Code	M	Used as defined in [RFC4006].
Final-Unit-Indication	-	Not used in WiMAX.
Final-Unit-Action	-	
Restriction-Filter-Rule	-	
Filter-Id	-	
Redirect-Server	-	
Redirect-Address-Type	-	
Redirect-Server-Address	-	
Check-Balance-Result	O _c	This field contains the balance checking result.
Credit-Control-Failure-Handling	O _c	Used as defined in [RFC4006].
Direct-Debiting-Failure-Handling	O _c	Used as defined in [RFC4006].
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.

PCC

AVP	Category	Description
Redirect-Host-Usage	O _C	Used as defined in [RFC3588].
Redirect-Max-Cache-Time	O _C	Used as defined in [RFC3588].
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 parameters.
R3-OC-Session-Continue	O _M	
AVP	O _C	

Note: See TS32.240-720 [7] for the meaning of "OM" and "OC".

9.6.2 Mobility handling

The procedure for mobility handling is in the scope of PCC-R3-OC specification [chapter 8.6.4]. 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.

9.7 PCC-R3-OC and PCC-R3-OFC AVP definitions

In the definition of the Diameter AVPs, AVPs that are specified in the referenced specifications but not used by the WiMAX charging specifications are marked with strikethrough.

9.7.1 Common AVPs used for WiMAX offline and online charging

This section describes Diameter AVPs that can be used in the WiMAX offline and online charging.

9.7.1.1 Service-Information

The *Service-Information* AVP (AVP code 873) is of type Grouped. Its purpose is to allow the transmission of additional 3GPP service specific information elements which are not described in this document.

It has the following ABNF grammar:

```
Service-Information ::= < AVP Header: 873 >
    { Subscription-Id }
    { PS-Information }
    { WLAN-Information }
    [ IMS-Information ]
    { MMS-Information }
    { LCS-Information }
    { PoC-Information }
    { MBMS-Information }
    { SMS-Information }
    [ Service-Generic-Information ]
    [ WiMAX-Information ]
```

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.

9.7.1.2 WiMAX-Information AVP

The *WiMAX-Information* AVP (AVP code 409) is of type Grouped and contains WiMAX access network accounting information for the offline and online charging.

It has the following ABNF grammar:

```
<WiMAX-Information> ::= < AVP Header: 409 >
    [ Acct-Session-Id ]
    [ Acct-Multi-Session-Id ]
    [ Acct-Delay-Time ]
    [ NAS-Identifier ]
    [ NAS-Port-Type ]
    [ Class ]
    [ Termination-Cause ]
    [ Accounting-Input-Octets ]
    [ Accounting-Input-Packets ]
    [ Accounting-Output-Octets ]
    [ Accounting-Output-Packets ]
    [ Acct-Link-Count ]
    [ Acct-Session-Time ]
    [ Calling-Station-Id ]
    [ Framed-IP-Address ]
    [ Framed-IPv6-Prefix ]
    [ Framed-Interface-Id ]
    [ CUI ]
    [ Session-Continue ]
    [ Beginning-Of-Session ]
    [ IP-Technology ]
    [ Hotline-Indicator ]
```

PCC

```

1          [ Hotlining-Capabilities ]
2          [ Prepaid-Indicator ]
3          [ Idle-Mode-Transition ]
4          [ Count-Type ]
5          [ hHA-IP-MIP4 ]
6          [ hHA-IP-MIP6 ]
7          [ NAP-ID ]
8          [ NSP-ID ]
9          [ BS-ID ]
10         [ Location ]
11         [ GMT-Time-Zone-Offset ]
12         [ Active-Time ]
13         [ Control-Packets-In ]
14         [ Control-Packets-Out ]
15         [ Control-Octets-In ]
16         [ Control-Octets-Out ]
17         * [ Uplink-Flow-Description ]
18         * [ Downlink-Flow-Description ]
19         [ Uplink-Granted-Qos ]
20         [ Downlink-Granted-Qos ]
21         [ Visited-Framed-IP-Address ]
22         [ Visited-Framed-IPv6-Prefix ]
23         [ Visited-Framed-Interface-Id ]
24         [ Direction ]
25         [ Interim-Cause ]
26         [ WiMAX-QoS-Information ]
27         [ AF-Correlation-Information ]
28         [ AF-Charging-Identifier ]
29         [ Access-Network-Charging-Identifier-Gx ]
30         [ Access-Network-Charging-Address ]
31         [ R3-OC-Session-Continue ]
32         [ Old-Session-Id ]
33         [ Offline-Charging ]
34
35

```

9.7.1.3 AF-Charging-Identifier

The *AF-Charging-Identifier* AVP (AVP Code 505) is of type OctetString and identifies a service data session, e.g. VoIP call. By AAA, this AVP is set to the value of SDFID AVP from the PCC-R3-OFC interface. For pre-provisioned SF, its SDFID is set to the value of AF-Charging-Identifier for the PCC-R3-OC interface.

AF-Charging-Identifier Mapping:

AF Charging Identifier [3][5] is generated by the AF and sent to PCEF through Rx and Gx interface. This information may be used for charging correlation with access layer. In WiMAX, AF charging Identifier is mapped to SDFID in offline charging interface. When A-PCEF/Accounting Client receives the AF-Charging-Identifier in the Charging-Rule-Definition AVP, it assigns the AF charging Identifier to the WiMAX SDFID attribute.

9.7.2 Offline Charging specific AVPs

9.7.2.1 Access-Network-Charging-Identifier-Value

The *Access-Network-Charging-Identifier-Value* AVP (AVP Code 503) is of type OctetString and identifies an IP-CAN bearer. By AAA, this AVP is set to the value of PDFID AVP from the PCC-R3-OFC interface.

9.7.2.2 Access-Network-Charging-Address

The *Access-Network-Charging-Address* AVP (AVP Code 501) is of type Address and indicates the IP address of the network entity within the access network performing charging. By AAA, this AVP is set to the value of NAS-IP-Address or NAS-IPv6-Address AVP from the PCC-R3-OFC interface.

9.7.2.3 SDFID

The *SDFID* AVP (AVP Code 27) as specified in [11] is of type OctetString and matches all packet data flows from the same service data flow. For dynamic SF, SDFID is set to the value of AF-Charging-Identifier AVP that is transmitted from PCRF.

9.7.2.4 PDFID

The *PDFID* AVP (AVP Code 26) as specified in [11] is of type OctetString and matches all records from the same packet data flow. For ISF and PPSF, PDFID is assigned by the CSN. For Dynamic SF, PDFID is set to the value of Access-Network-Charging-Identifier-Value that is assigned by the ASN. PDFID SHALL be assigned to be unique in an IP-session and remains constant through all handover scenarios.

9.7.2.5 Uplink-Flow-Description

The *Uplink-Flow-Description* AVP (AVP Code 50) is of type IPFilterRule and describes an Uplink PD flow with the header fields.

9.7.2.6 Downlink-Flow-Description

The *Uplink-Flow-Description* AVP (AVP Code 62) is of type IPFilterRule and describes a Downlink PD flow with the header fields.

9.7.2.7 Uplink-Granted-QoS

The *Uplink-Granted-QoS* AVP (AVP Code 30) is of type Grouped and specifies Uplink QoS granted to the MS.

It has the following ABNF grammar:

```
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 ]
```

9.7.2.8 Downlink-Granted-QoS

The *Downlink-Granted-QoS* AVP (AVP Code 63) is of type Grouped and specifies Downlink QoS granted to the MS.

It has the following ABNF grammar:

```
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-InSDP-Format ]
    [ Transmission-Policy ]
    [ Unsolicited-Grant-Interval ]
    [ SDU-Size ]
```

9.7.2.9 Direction

The *Direction* AVP (AVP code 306) as specified in [11] is of type Enumerated and indicates the direction of the packet data flow.

9.7.2.10 Charging-Information

The *Charging-Information* AVP (AVP Code 618) is of type Grouped and contains the addresses of the charging functions such as the OCS and the OFCS. The OCS and OFCS addresses may be pre-configured at the AAA. In the PCC based charging, however, if the AAA receives this Grouped AVP from the PCEF, then it SHALL use the OCS or the OFCS address (of type DiameterURI) included in this AVP. For offline charging, Primary/Secondary-Charging-Collection-Function-Name AVPs containing the OFCS address are used. This Grouped AVP is not forwarded to the OFCS over PCC-R3-OFC' interface.

It has the following ABNF grammar:

```
Charging-Information ::= < AVP Header: 618 >
    [ Primary-Event-Charging-Function-Name ]
    [ Secondary-Event-Charging-Function-Name ]
    [ Primary-Charging-Collection-Function-Name ]
    [ Secondary-Charging-Collection-Function-Name ]
    * [ AVP ]
```

9.7.3 Online Charging specific AVPs

9.7.3.1 Multiple-Services-Credit-Control AVP

The Multiple-Services-Credit-Control AVP (AVP code 456) is of type grouped as specified in IETF RFC 4006 [16] and extended by TS32.299 [9]. 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 [9] needs to be provided.

PCC

1 It has the following ABNF grammar:

```

2      Multiple-Services-Credit-Control ::= < AVP Header: 456 >
3                                     [ Granted-Service-Unit ]
4                                     [ Requested-Service-Unit ]
5                                     * [ Used-Service-Unit ]
6                                     — [ Tariff-Change-Usage ]
7                                     * [ Service-Identifier ]
8                                     [ Rating-Group ]
9                                     * [ G-S-U-Pool-Reference ]
10                                    [ Validity-Time ]
11                                    [ Result-Code ]
12                                    [ Final-Unit-Indication ]
13                                    [ Time-Quota-Threshold ]
14                                    [ Volume-Quota-Threshold ]
15                                    [ Unit-Quota-Threshold ]
16                                    [ Quota-Holding-Time ]
17                                    [ Quota-Consumption-Time ]
18                                    * [ Reporting-Reason ]
19                                    [ Trigger ]
20                                    — [ PS-Furnish-Charging-Information ]
21                                    * [ AF-Correlation-Information ]
22                                    * — [ Envelope ]
23                                    — [ Envelope-Reporting ]
24                                    [ Time-Quota-Mechanism ]
25                                    * [ AVP ]
26
```

27 9.7.3.2 Hotlining-Capabilities

28 This AVP if FFS.

29 9.7.3.3 Hotlining- Indicator

30 This AVP if FFS.

10. Handling Error Cases

This section describes how to handle various error cases in PCC. In this document, the error cases include only those that can occur between SFA/A-PCEF and PDF/PCRF.

10.1 Types of Error Cases

Typical types of error cases are defined.

10.1.1 Disconnection with peer entity – Type I

In this case of failures, due to the disconnection between a server and a client, they cannot send any request to the peer.

- WiMAX IP-CAN session establishment failure: depending on operator's policy the MS either exits the network or is connected without subsequent PCC interactions (i.e., no dynamic QoS service for the IP-CAN session).
- WiMAX IP-CAN session modification failure: both sides will not be able to update the state of the IP-CAN session. State inconsistency may happen between A-PCEF and PDF/PCRF. For example, different states after removal of some of bearers (or PCC rules) could affect service quality (or waste air resource).
- WiMAX IP-CAN session termination failure: In case of MS or A-PCEF initiated, the MS network exit procedure will not wait for successful IP-CAN session termination procedure PCC. Regardless of failure, network exit procedures will have to proceed. The A-PCEF will be aware of the MS' network exit and can remove all IP-CAN session information. To avoid state inconsistency the PCRF must also learn about the MS' network exit and remove all IP-CAN session information. How the PCRF learns this is outside the scope of this specification.

How to synchronize states between SFA/A-PCEF and PDF/PCRF after the communication is resumed is described in section 10.3.

10.1.2 Delayed or no response (timeout) – Type II

This type of error happens when processing a request (e.g., PCC rule enforcement) is delayed or is malfunctioned so that the sender will not receive any response within a given timeout period. Unlike the above case (Type I), the system may retry the request if the system finds it worthwhile. Possible delayed response cases include:

- Diameter CCA timeout or Radius Access-Request timeout
- RAA timeout or Radius COA/DM timeout

10.1.3 Response with failure result – Type III

In order to enforce PCC rules, SFA/A-PCEF needs to interact with other entities. For example, SFA/A-PCEF has to send request(s) to SFM to create additional service flows for a MS. During the procedure, various error cases can happen. Therefore, the result of a response message may convey failure for the requested action (e.g. CCA or RAA with failure indication). Possible failure response cases include:

- Diameter CCA with failure
- Diameter RAA or Radius COA with failure

In order to avoid state inconsistency, the originator of a request with a failed result must roll back its state to remove the failed transactions.

10.2 General Principle

10.2.1 IP-CAN session establishment

It is obvious that the PCC based service is not applicable if the IP-CAN session establishment fails. However, there could be an operator which would like to provide Internet access service for the MS without PCC. For the failure of IP-CAN session establishment, the A-PCEF either initiates the network exit of the MS or triggers reauthentication with the HAAA, authorize only, and removes support for PCC in the WiMAX Capabilities AVP. If the HAAA reauthorizes service to the MS without PCC, the A-PCEF proceeds to the network entry procedure without PCC IP-CAN session. If the HAAA does not reauthorize service to the MS without PCC, the A-PCEF initiates network exit of the MS. These two scenarios are depicted in Annex F. 4.

The followings are major error reasons for the failure of IP-CAN session establishment.

- The failure of DIAMETER/RADIOUS connection (i.e., Type I Error)
- CCA timeout (i.e., Type II Error)
In this case, the A-PCEF may retry the IP-CAN session establishment procedure.
- CCA with failure (i.e., Type III Error)
Annex F. 3 shows flows for this example of error handling scenario.

Note that if the A-PCEF proceeds to the network entry procedure for the MS without establishing IP-CAN session, the MS will have only initial ISF/PPSFs and not able to receive dynamic QoS service via PCC.

10.2.2 IP-CAN session termination

In case of MS or A-PCEF initiated, the MS's network exit procedure will not wait for successful IP-CAN session termination procedure. This is because users simply trigger to close the application or turn off the power. Similarly, in the PCRF initiated (or AF initiated) cases, the PCRF could not wait for successful IP-CAN session termination procedure because AF has already been terminated the application session.

The followings are major error reasons for the failure of IP-CAN session termination.

- The failure of DIAMETER/RADIOUS connection (i.e., Type I Error).
This could happen in both A-PCEF initiated case and PCRF initiated case.
- CCA timeout (i.e., Type II Error)
- CCA with failure (i.e., Type III Error)

Regardless of failure reasons, network exit or IP-CAN session termination procedure will have to proceed. State inconsistency may occur for these cases.

10.2.3 IP-CAN session modification

This section describes the error handling for the failure of WiMAX IP-CAN session modification according to the criteria of section 10.1 Types of Error Cases.

10.2.3.1 The error handling of A-PCEF

The followings are major reasons for the IP-CAN session modification failure of A-PCEF.

- PCC rules install failure (e.g. Type III Error)
- PCC rule modify failure (e.g. Type III Error)
- PCC rule remove failure (e.g. Type III Error)

In the above cases, failure of the A-PCEF of PCC rules is reported to the PCRF on a per PCC rule basis [3]. The failed PCC rules are identified in the charging rule report along with a rule failure reason and put into the inactive state. This enables the PCRF to synchronize its state with that of the A-PCEF after rule failure. The subsequent actions to be taken by the PCRF due to the failed rules are based recommendations in [3] and on network and

PCC

operator policies and not further specified in this document. Annex F. 3 presents example message flows for the error handling of this scenario.

10.3 States Synchronization

The A-PCEF may have a different set of PCC rules from those of the PDF/PCRF without knowing it each other due to various reasons including absence of response, delayed response, and changes happened during the temporary disconnection period. In order to resolve the inconsistency of states, the A-PCEF finds any suspicious PCC rules or IP-CAN sessions to be re-authorized by the PDF/PCRF and then sends CCR messages. Finding suspicious PCC information is outside the scope of this document and it is optional to implement. The support of this feature is per operator's policy.

10.3.1 Reporting PCC Rules Status

In order to report the status of PCC rules during the synchronization, Charging-Rule-Report AVP shall be utilized in the CCR message. Within the Charging-Rule-Report AVP, the PCC-Rule-Status AVP is used to describe the status of PCC rule(s), for example, active or inactive.

10.3.2 States Synchronization Flow

Figure 21 depicts the procedure of states synchronization. An example of solving states inconsistency is shown in Annex F. 4.

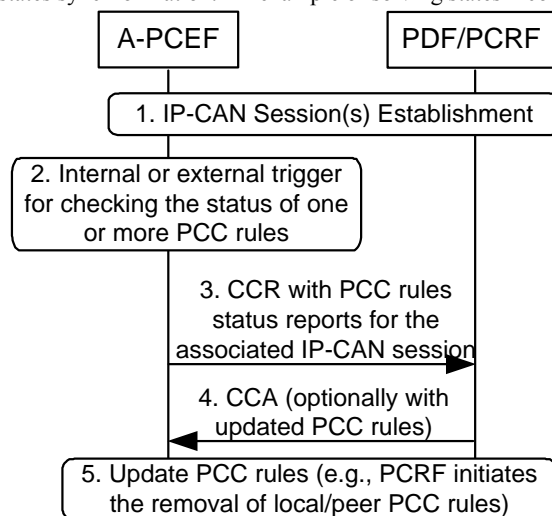


Figure 21: States Synchronization Flow

- 1 The A-PCEF and the PDF/PCRF have established one or more IP-CAN session.
- 2 The A-PCEF is triggered by an internal or external event to check the status of one or more PCC rules. For example, the A-PCEF searches every day at midnight for PCC rules which have been for over an hour.
- 3 The A-PCEF sends a CCR message for the IP-CAN session with Event-Trigger AVP set to "PCC_RULE_REAUTHORIZATION." The CCR command shall include Charging-Rule-Report AVP in which each PCC rule's status is reported. The CC-Request-Type AVP shall be set to the value "UPDATE_REQUEST."
- 4 The PDF/PCRF then acknowledge to the request by sending a successful CCA message. The CCA message may optionally convey updated PCC rules. Or, the updated rules may be provided in a following RAR message as shown in Step 5.

PCC

- 1 5 The PDF/PCRF may initiate the removal of local PCC rules which does not exist in the A-PCEF, or
2 may send a RAR command to the A-PCEF in order to remove PCC rules which have been already
3 removed in the local but remain in the A-PCEF.
4

5 **10.1 Failure Code**

- 6 Proper error handling requires appropriate failure codes and reasons. Some cases of failure will use the Result-Code
7 AVP values defined in Diameter BASE RFC 3588 [18] and some others the Gx and PCC-R3-P specific
8 Experimental-Result-Code AVP values. Refer to 3GPP TS 29.212 [3] and Diameter base protocol [18] for failure
9 reason values and the complete list of failure result codes.

10

Annex A Interworking with 3GPP PCC

Interworking is not specified in this release of the document.

Annex B Interworking with 3GPP2 PCC

Interworking is not specified in this release of the document.

Annex C Roaming Architecture with HA in the Visited Network

Figure 22 illustrates the WiMAX policy control roaming architecture with the HA in the visited network.

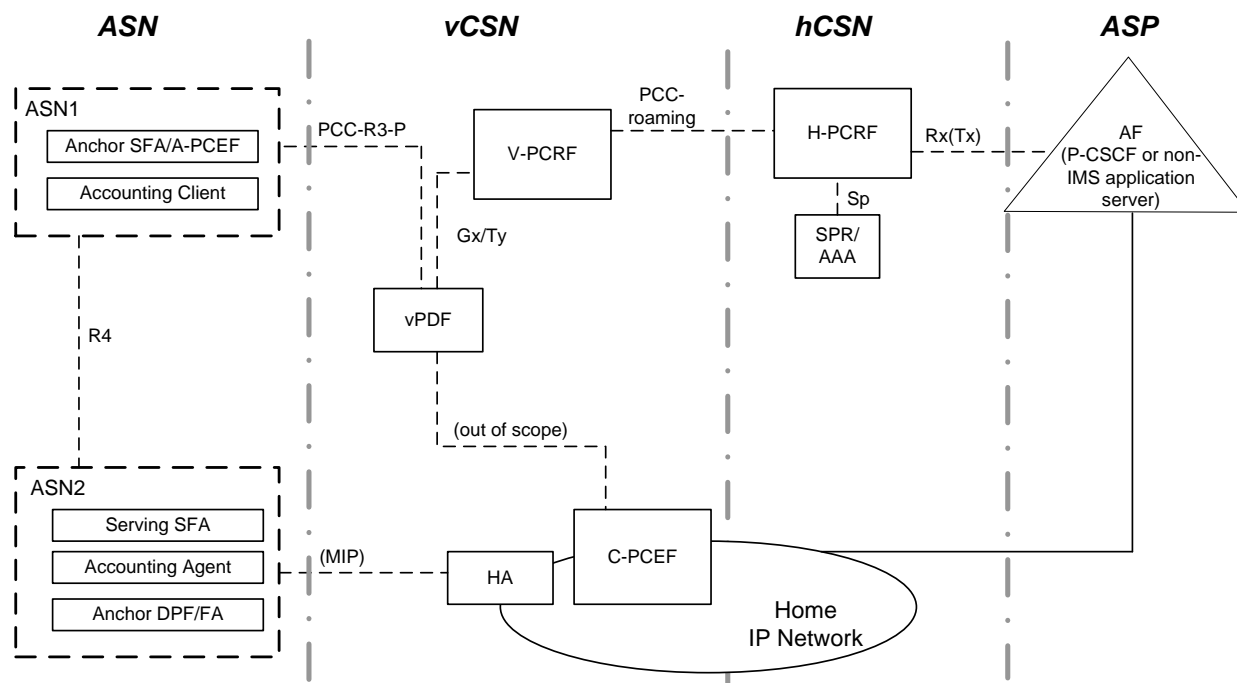


Figure 22: WiMAX PCC roaming architecture with HA in the visited network

Annex D QoS Mapping (Informative)

Table 15: Recommended QoS parameters translation

3gpp QCI	WiMAX Type of Data Delivery Services	Traffic Priority	Max Latency msec	Expected Packet Loss Rate	Reduced Resources Code
1 [a]	UGS	0	50	1	No
1 [b]	eRT-VR	0	50	1	No

1 [c]	RT-VR	6	50	1	No
2	RT-VR	4	50	2	No
3	RT-VR	2	250	3	No
4	RT-VR	6	50	6	Yes
5	RT-VR	4	50	3	Yes
6	NRT-VR	2	250	4	Yes
7	NRT-VR	4	250	6	Yes
8	BE	2	500	6	Yes
9	BE	0	N/A	N/A	N/A

WiMAX scheduling type and some other parameters (fixed values) are derived from QCI values in a limited way as presented in Table 15. The recommended WiMAX scheduling types (types of data delivery services) to be used when translating the QCI, cover all service types provided by WiMAX, i.e., UGS, eRT-VR, RT-VR, NRT-VR and BE. The support of the data delivery services UGS and eRT-VR is optional and depends on whether the Grant Interval and/or Packet-Size (defined as an optional extension to the 3GPP QoS-Information AVP) are supported by the PDF and/or the PCRF or ASN. In case of a separated PDF implementation vendor specific attributes can be used between PDF and PCRF to support UGS and/or eRT-VR. Reduced Resource Code TLV differentiates between “service blocking over service dropping” (as specified in [19] for GBR vs. non-GBR traffic types – i.e. rather block a service request than risk degraded performance of an already admitted service request). Fixed values of Maximum Latency are assumed for translated QoS descriptor. Use of other WiMAX-specific QoS parameters, not listed in Table 15, when translating Authorized-QoS AVP is implementation specific.

Notes:

[a] The QCI represents “UGS” if packet-size & packet interval are included in the QoS-Information AVP

[b] The QCI represents “eRT-VR” if packet interval only included in the QoS-Information AVP

[c]: The QCI represents “RT-VR”. Neither packet-size nor packet interval need to be included in the QoS-Information AVP

Annex E ASN Procedures for Interworking with PCC Framework (Informative)

Note: the Simple IP scenarios are not covered in this Annex.

E. 1 Session establishment

Figure 23 presents intra-ASN message flow for initial IP-CAN session establishment, which corresponds to the PCC-R3 message flow described in the Section 8.2. The figure presents PMIP scenario with Anchor DP acting as DHCP Relay Agent. Other scenarios, such as CMIP/ Simple IP are possible also.

An A-PCEF context is created per-MS in the same ASN entity as Authenticator, Anchor SFA and AAA Client. During Initial Network Entry the above functional entities are collocated with Serving SFA, Anchor DP and FA.

Note, that IP Host may be a separate entity behind WiMAX MS/ SS. In such scenarios DHCP procedure may occur some time after WiMAX MS/ SS completes initial access authentication, network registration and is provided with ISF/ PPSFs.

Figure 23 below presents an example message flow for PMIP scenario.

PCC

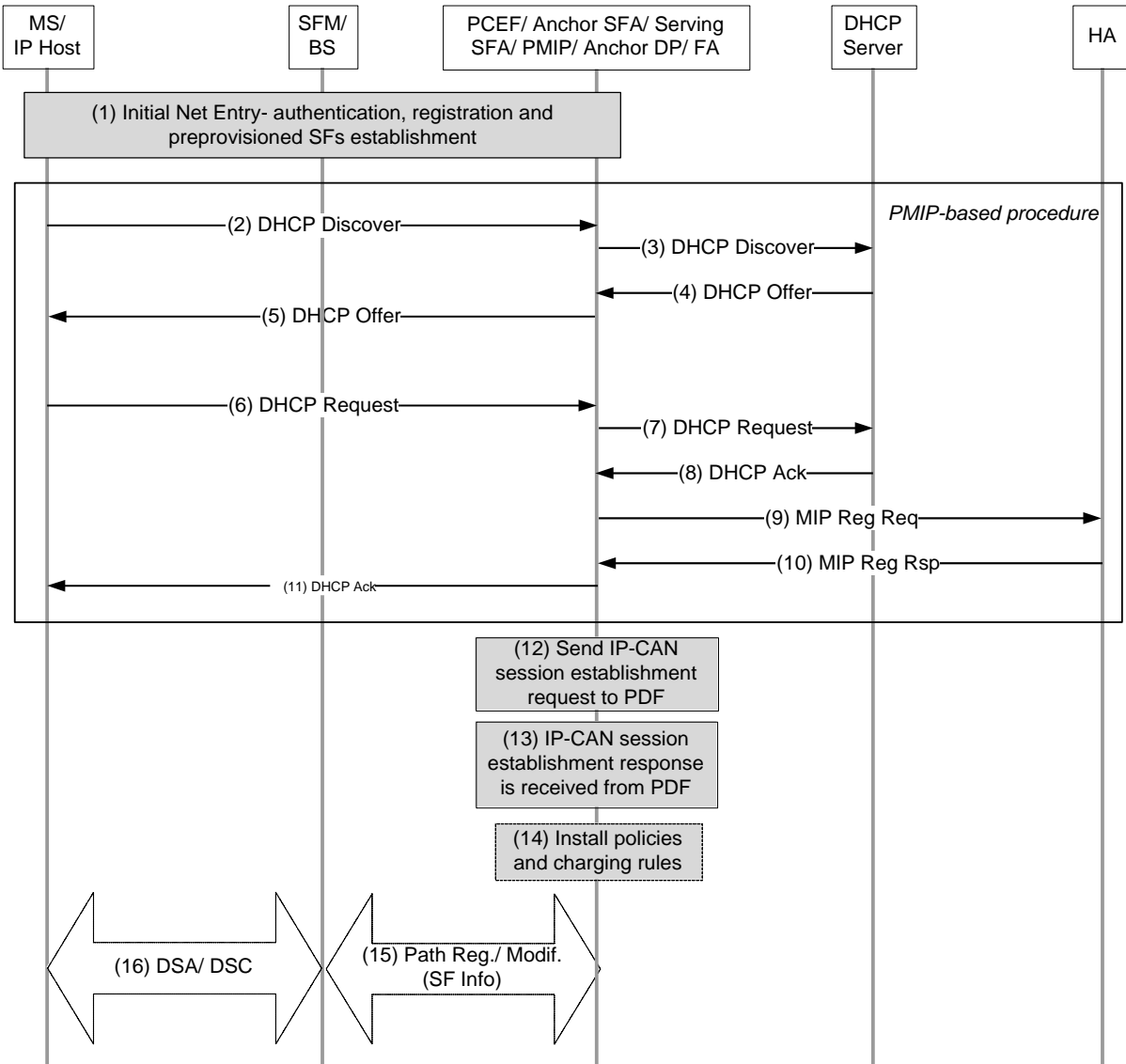


Figure 23: ASN procedures for IP-CAN session establishment

1. WiMAX MS/ SS performs initial network entry including initial access authentication and network registration. As a result, network establishes a data path for the MS/ SS – creates Initial Service Flow(s) or optionally all the Preprovisioned Service Flows.
2. IP Host initiates IP address allocation process. In the PMIP/ Simple IP scenario, it sends DHCP Discover message. This message is delivered over the pre-established data path to the Anchor DP functional entity.
3. Anchor DP entity intercepts DHCP Discover broadcast and invokes a DHCP Relay Agent relaying DHCP Discover message to DHCP server.
4. DHCP Server responds with DHCP Offer message including an offered IP address.
5. DHCP Relay Agent/ Anchor DP relays DHCP Offer message to IP Host over the pre-established data path.
6. IP Host sends DHCP Request message confirming its choice of the DHCP Server.
7. Anchor DP/ DHCP Relay Agent relays DHCP Request message to DHCP Server.
8. DHCP Server responds with DHCP Ack message.

PCC

9. DHCP Relay Agent prompts PMIP Client to initiate MIP registration. PMIP Client constructs MIP Registration Request and on behalf of FA sends it to HA.
 10. HA responds with MIP Registration Reply message.
 11. PMIP Client provides DHCP Relay Agent with results of MIP registration. DHCP Relay Agent/ Anchor DP relays DHCP Ack message to IP Host over the pre-established data path.
 12. A-PCEF detects completion of IP address allocation procedure and starts IP-CAN session establishment with PDF/ PCRF.
 13. PDF/ PCRF confirm IP-CAN session establishment and optionally may include new PCC rules in the response message.
 14. If new policies are provided by PDF/ PCRF in the previous step, A-PCEF/ Anchor SFA perform “bearer binding” operation and invoke the collocated Serving SFA/ Acct Agent to install the corresponding policies and charging rules. Optionally, if only ISF(s) has been established in step (1), Anchor SFA may initiate PPSF establishment.
 15. If Anchor SFA initiates WiMAX Service Flow operations, Serving SFA should communicate this across the data path with SFM over R6.
 16. If over-the-air resource reservation/ allocation is requested, SFM may apply admission control procedure. If the request is admitted, SFM performs over-the-air Service Flow operation (DSx transaction) and responds back to Serving SFA.
- Note that Acct Update is not presented on this flow.

E. 2 Session termination

IP-CAN session termination procedure may be triggered by either MS Network Exit (WiMAX authentication session termination) or by IP address release (DHCP release or MIP session release). Different ASN and CSN entities may instigate MS Network Exit or IP address release (refer to [11]). The below subsections present some examples of such scenarios.

E.2.1 MS/BS initiated

Figure 24 presents intra-ASN message flow for MS or BS initiated Network Exit resulting in IP-CAN session termination. This flow corresponds to the PCC-R3 message flow described in the Section 8.3.1.

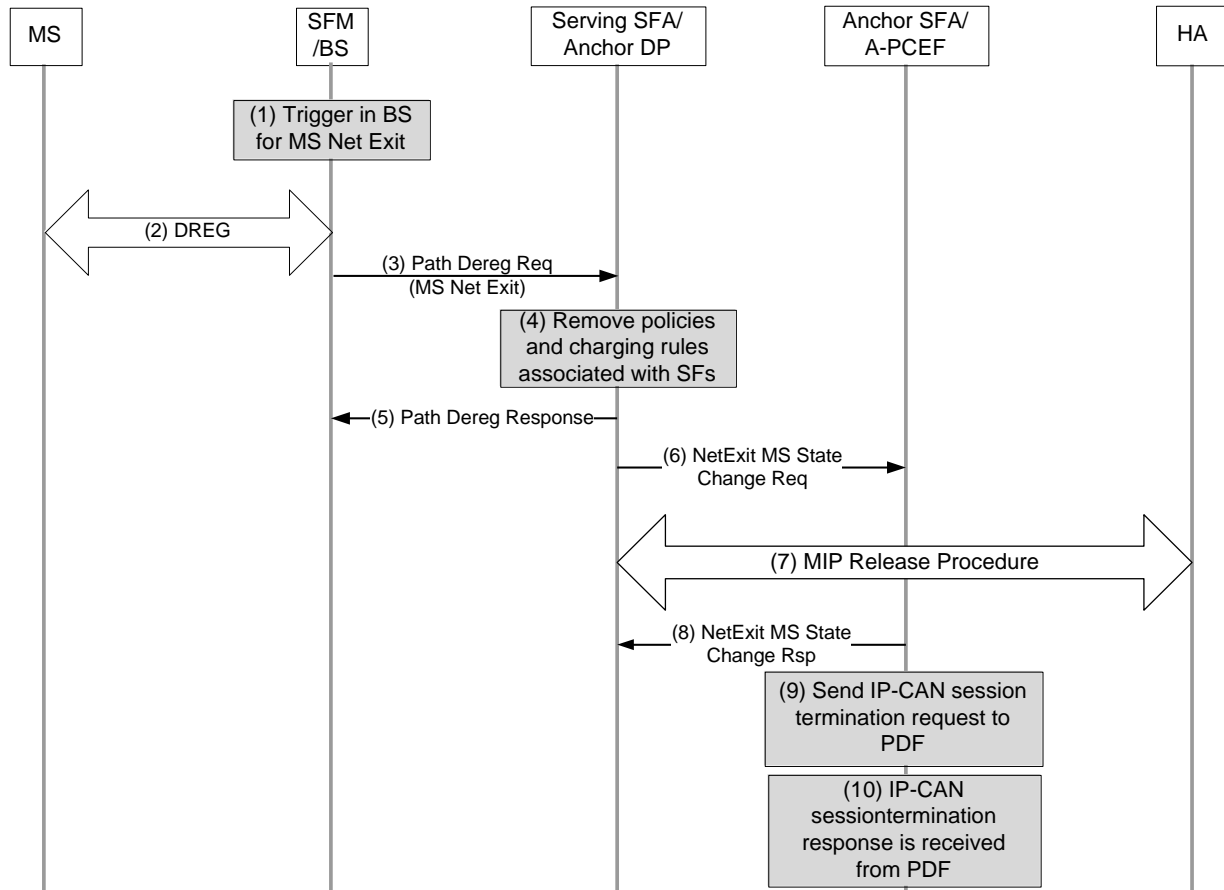


Figure 24: ASN procedures for MS/ BS-initiated session release (Network Exit)

1. This step presents BS trigger for MS deregistration from the network (Network Exit). In the case of MS-initiated Network Exit, this step is omitted.
 2. MS or BS initiate over-the-air MS deregistration transaction.
 3. Serving BS initiates data path removal procedure by sending *Path Dereg Req* message with Network Exit Indicator along the data path to Anchor DP/ Serving SFA. This step occurs when BS detects the completion of over-the-air MS deregistration procedure.
 4. Serving SFA/ Acct Agent remove policies and charging rules associated with the corresponding data path(s)/ service flow(s) for the MS.
 5. Anchor DP entity confirms path deregistration to Serving BS.
 6. Serving SFA/ Anchor DP signals MS Network Exit to Authenticator by sending *NetExit MS State Change Req* message including Network Exit Indicator TLV. For CMIP, FA collocated with Anchor DP, performs MIP Revocation procedure.
 7. For PMIP, the PMIPv4 client collocated with Authenticator can perform MIP De-Registration procedure.
 8. Authenticator responds with *NetExit MS State Change Rsp* message to Anchor DP.
 9. A-PCEF collocated with Authenticator detects release of WiMAX session and initiates IP-CAN session termination by sending a request message to PDF/ PCRF. If there are multiple IP hosts behind the same WiMAX MS/ SS, all the IP addresses are impacted and all IP-CAN session shall be released.
 10. PDF/ PCRF confirms IP-CAN session termination.
- Note that Acct Update is not presented on this flow.

PCC

E.2.2 MS initiated IP address release

Figure 25 presents intra-ASN message flow for MS initiated IP address release (PMIPv4 scenario) resulting in IP-CAN session termination.

There are other triggers that may cause IP session release – e.g. IP address lease time expiry or FA-initiated session release, etc.

This flow corresponds to the PCC-R3 message flow described in Section 8.3.1.

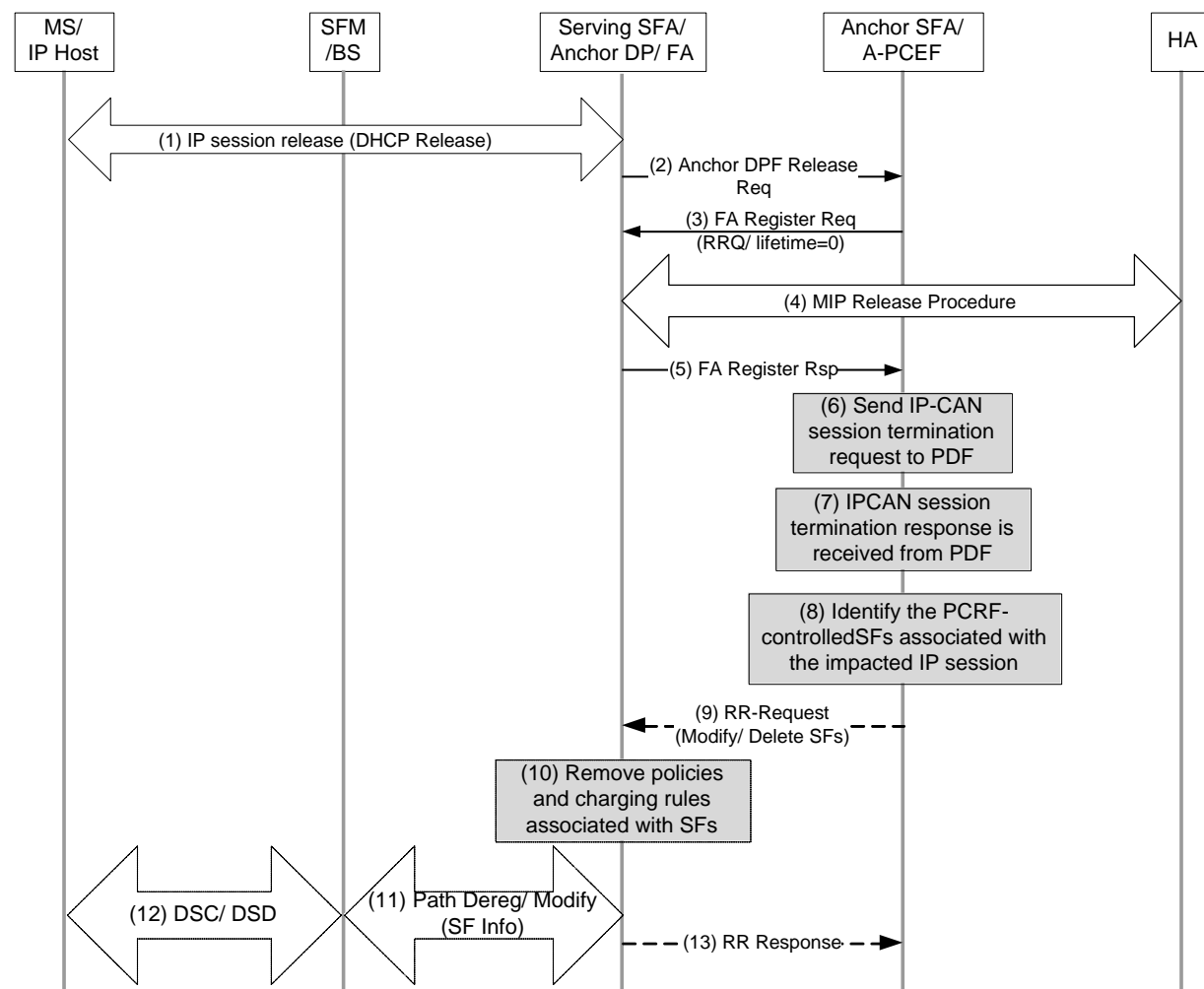


Figure 25: ASN procedures for IP Host initiated session release

1. IP Host entity initiates IP address release (DHCP Release). This message is delivered through the MS' data path to Anchor DP/ DHCP Proxy functional entity in ASN (collocated with Serving SFA, FA and Acct Agent entities).
2. Anchor DP function initiates the session release with PMIPv4 client (collocated with Authenticator/ Anchor SFA/ Acct Client and A-PCEF entities) by sending *Anchor DPF Release Req* message.
3. PMIPv4 Client sends *FA Register Req* message to Anchor DP/ FA entity including MIP RRQ with lifetime=0.
4. FA entity proceeds with MIP session release procedure with the HA.
5. Anchor DP/ FA receiving RRP from the HA sends *FA Register Rsp* message including MIP RRP to PMIPv4 Client.

PCC

- 1 6. PMIPv4 Client receiving *FA Register Rsp* invokes the collocated A-PCEF entity indicating IP session
2 release completion. A-PCEF initiates IP-CAN session termination by sending a request message to PDF/
3 PCRF.
- 4 7. PDF/ PCRF confirms IP-CAN session termination.
- 5 8. A-PCEF/ Anchor SFA entity identifies the PCC rules and the PCRF-controlled WiMAX Service Flows
6 associated with the impacted IP-CAN session. Anchor SFA initiates removal of these PCC rules (associated
7 with PCRF-controlled Service Flows). When the last IP session is terminated, Anchor SFA switches to
8 Preprovisioned Service Flows as specified by HAAA during initial network entry.
- 9 9. If, as a result of the previous step, some changes are required for WiMAX Service Flows (Service Flow
10 modification or deletion), Anchor SFA entity signals these changes to Serving SFA/ Anchor DP using *RR-*
11 *Request* message with SF Info compound TLVs. Note, that steps 9-13 are optional for the case when A-
12 PCEF/ Anchor SFA identifies WiMAX Service Flows impacted by IP session termination.
- 13 10. Serving SFA/ Anchor DP removes policies and charging rules associated with impacted Service Flows as
14 requested in *RR-Request* message.
- 15 11. Anchor DP initiates modification/ deletion of the data path associated with the impacted Service Flows
16 using Path Modification/ Deregistration messages.
- 17 12. Serving BS performs the corresponding changes over-the-air using DSC/ DSD transactions.
- 18 13. When Anchor DP/ Serving SFA receives response message for data path modification/ deletion, it sends
19 *RR-Response* message to Anchor SFA indicating completion of the requested operation.
- 20 Note that Acct Update is not presented on this flow.

21 E.2.3 A-PCEF initiated

22 Figure 26 presents intra-ASN message flow for A-PCEF initiated Network Exit resulting in IP-CAN session
23 termination. Note that A-PCEF is collocated with other ASN functional entities – e.g. Authenticator, which may
24 trigger MS Network Exit (A-PCEF entity by itself does not instigate MS Network Exit).

25 This flow corresponds to the PCC-R3 message flow described in the Section 8.3.2.

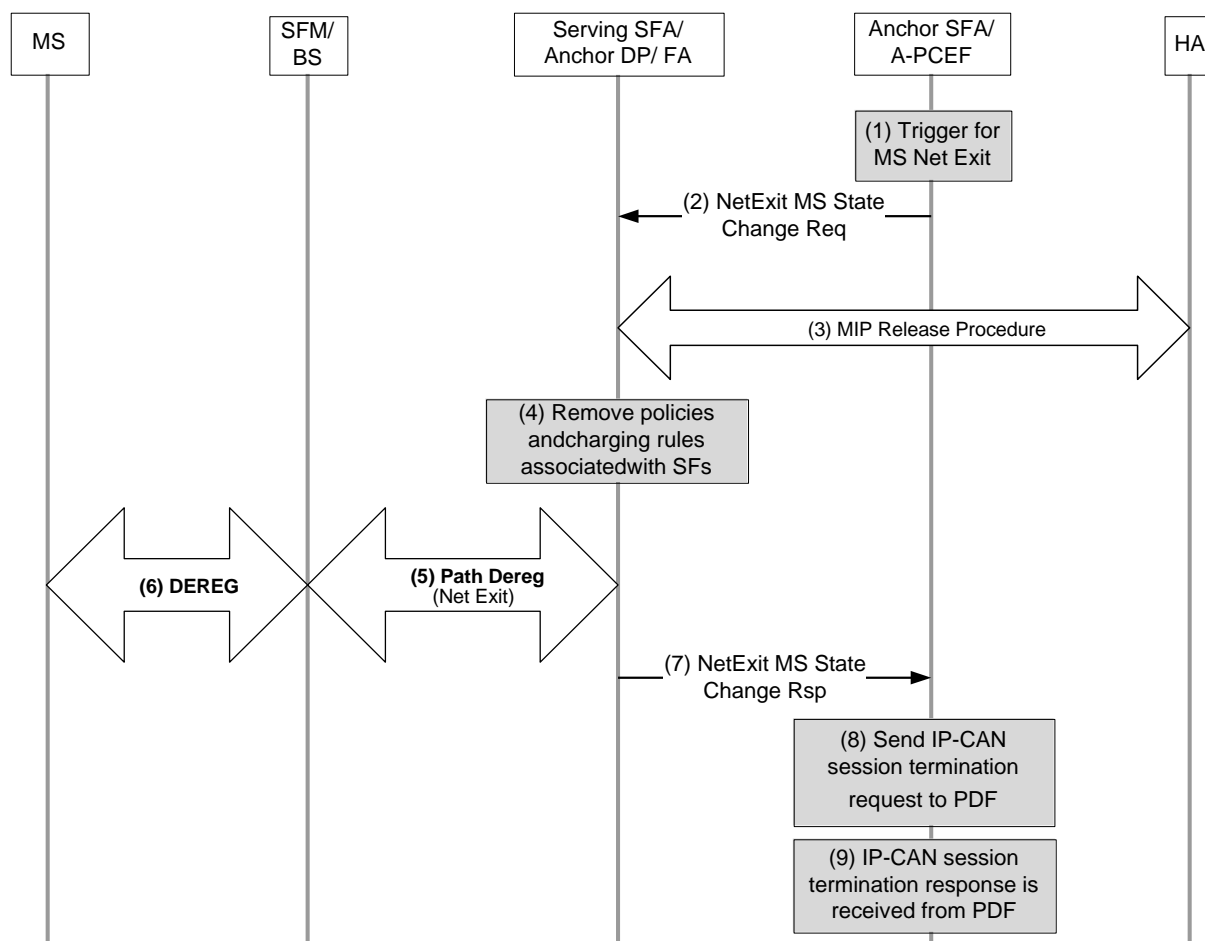


Figure 26: ASN procedures for A-PCEF initiated session release

1. MS Network Exit trigger occurs in the ASN entity where A-PCEF is located. E.g. it may be MS' Authenticator that initiates MS Network Exit for some reason.
2. Authenticator proceeds with the MS Network Exit process by sending *NetExit_MS_State_Change_Req* message to Anchor DP entity (as one of the options; otherwise, it may use this message triggering MS Network Exit in Serving BS)
3. For PMIP, the PMIP Client collocated with Authenticator can perform MIP De-Registration procedure. For CMIP, it is either triggered by CMIP client when MS receives deregistration indication in step (6) or, otherwise, FA performs MIP Revocation procedure in step (7).
4. Serving SFA/ Acct Agent, collocated with Anchor DP entity remove policies and charging rules associated with the MS' corresponding data path(s)/ service flow(s). This step occurs when bearer path for the specific IP session becomes unavailable – either MIP tunnel or R4/ R6 data path for the session is terminated. If PMIP session is not released in step (3), then this step occurs either in step (6) if CMIP session is released by CMIP client or in step (7) when Anchor DP receives indication from SBS that path deregistration is complete.
5. Anchor DP entity proceeds with data path deregistration for the impacted MS using *Path Deregistration* messages with specific network exit indication.
6. Serving BS receiving MS Network Exit indication proceeds with MS over-the-air deregistration and responds back to Anchor DP with *Path Deregistration Rsp* message.
7. Anchor DP terminates the data path and confirms MS Network Exit to Authenticator by sending *NetExit MS State Change Rsp* message.

PCC

8. A-PCEF collocated with Authenticator detects release of IP session and initiates IP-CAN session termination by sending a request message to PDF/ PCRF. If there are multiple IP hosts behind the same WiMAX MS/ SS, MS network exit will impact all the IP sessions for this MS.

9. PDF/ PCRF confirms IP-CAN session termination.

Note that Acct Update is not presented on this flow.

E.2.4 PCRF initiated

Figure 27 presents intra-ASN message flow for PCRF initiated IP-CAN session termination. Note that IP-CAN session termination does not necessary trigger WiMAX MS/ SS Network Exit or IP session termination (implementation specific). As a mandatory requirement, PCRF-initiated IP-CAN session termination removes PCC rules associated with the IP-CAN session.

This flow corresponds to the PCC-R3 message flow described in the Section 8.3.3.

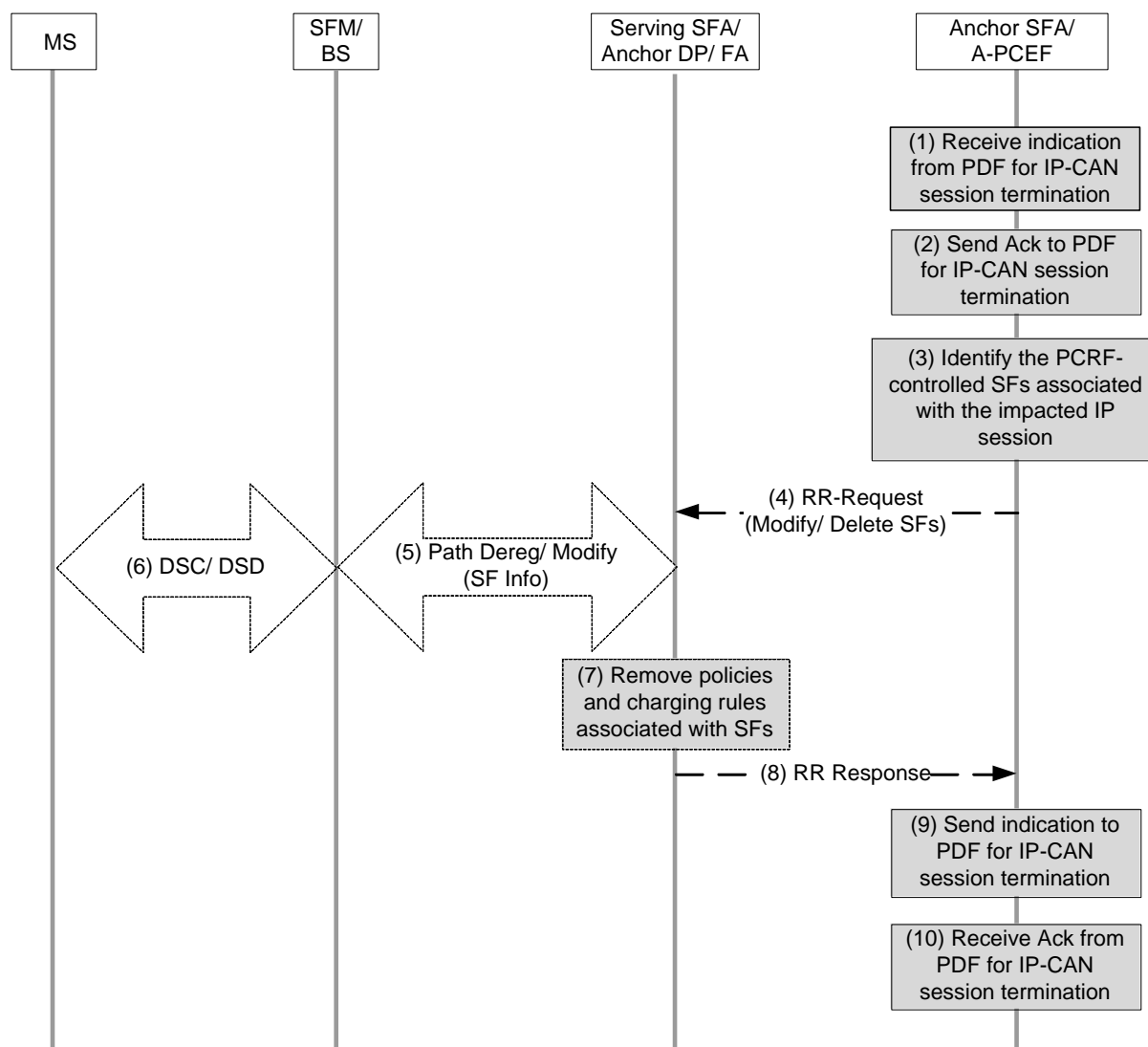


Figure 27: ASN procedures for PCRF initiated IP-CAN session release

1. A-PCEF receives a request from PDF/ PCRF for IP-CAN session termination.
2. If A-PCEF is able to identify the corresponding MS/ IP-CAN session, it acknowledges the request.

PCC

3. A-PCEF identifies active PCC rules provided by PCRF previously for this IP-CAN session. Other IP-CAN sessions that may be using the same bearer are not impacted. Note, that when PCRF-installed PCC rules are removed, Anchor SFA uses HAAA-provided flow descriptors for preprovisioned flows (Anchor SFA removes/ modifies dynamically controlled Service Flows, and switches to Preprovisioned Service Flows).
 4. If A-PCEF identifies PCRF-installed PCC rules associated with the impacted IP-CAN session, then it invokes collocated Anchor SFA entity to modify/ delete WiMAX Service Flows corresponding to these PCC rules (steps 4 – 8 are optional). Anchor SFA sends *RR-Request* message to Serving SFA entity with a request to delete/ modify dynamically controlled Service Flows.
 5. Serving SFA invokes the collocated Anchor DP entity, which initiates data path modification/ deletion for the corresponding Service Flows using *Path Modification / Deregistration* messages.
 6. Serving BS receiving a request for data path/ service flow modification or deregistration performs the corresponding over-the-air DSx transaction and responds back for data path modification/ deregistration completion.
 7. Anchor DP/ Serving SFA/ Acct Agent receiving indication that data path modification/ deregistration has been complete, remove policies and charging rules associated with the corresponding Service Flows.
 8. Serving SFA indicates Service Flow modification/ deregistration completion to Anchor SFA using *RR-Response* message.
 9. Anchor SFA invokes the collocated A-PCEF and the latest sends indication for IP-CAN session termination to PDF/ PCRF.
 10. PDF/ PCRF acknowledges IP-CAN session termination.
- Note that Acct Update is not presented on this flow.

E. 3 Session modification

E.3.1 PCRF initiated

Figure 28 presents intra-ASN message flow for PCRF initiated IP-CAN session modification. Note that Admission Control module in SFM may reject some requests for operations with Service Flow(s), which require allocation of new resources over-the-air. A-PCEF communicates ASN admission control decision with PDF/ PCRF.

This flow corresponds to the PCC-R3 message flow described in the Section 8.4.1.

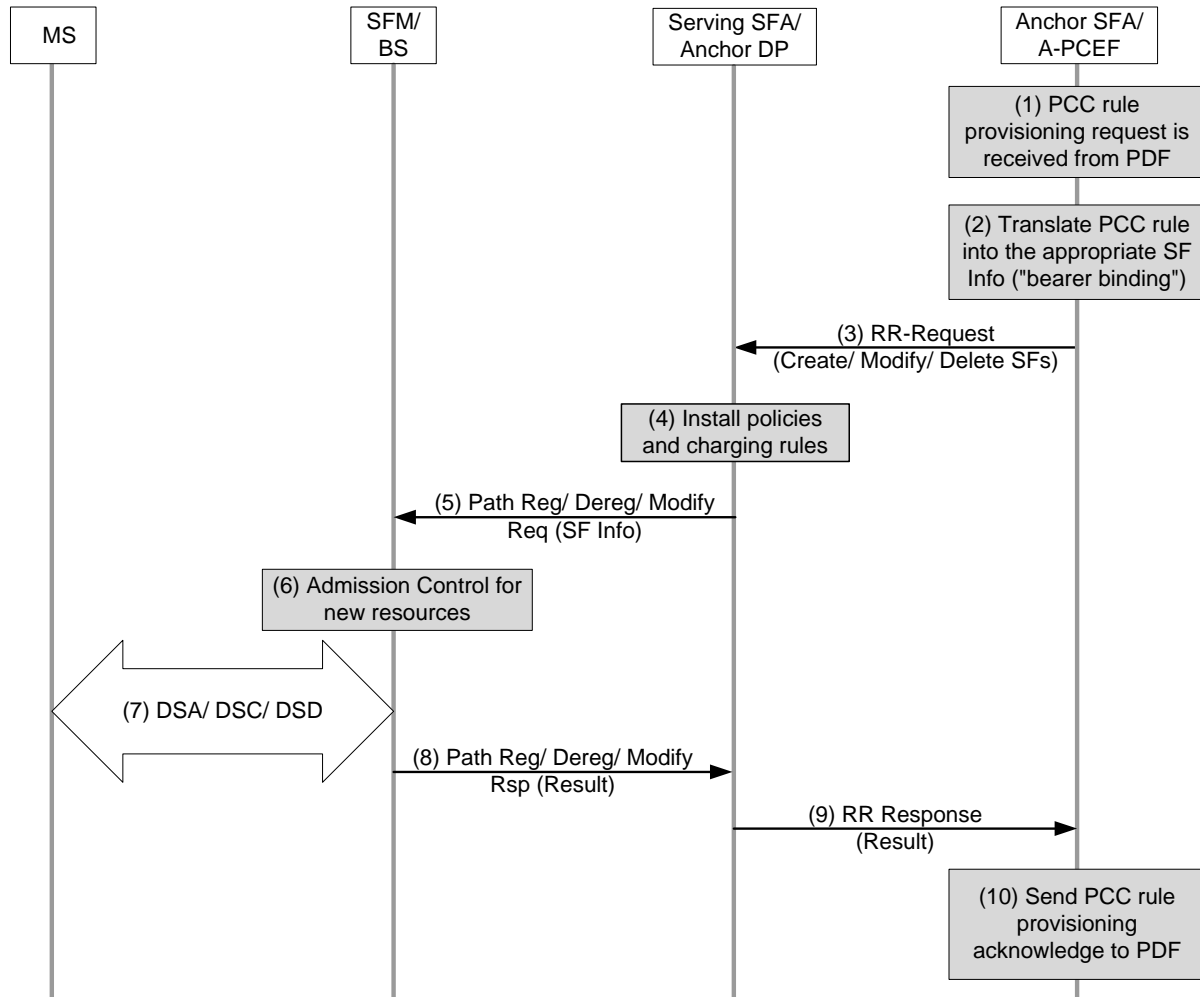


Figure 28: ASN procedures for PCRF initiated IP-CAN session modification

1. A-PCEF receives IP-CAN session modification request from PDF/ PCRF (PCC rule provisioning request).
2. A-PCEF performs “bearer binding” – associates the received PCC rule provisioning request with the corresponding operation for WiMAX Service Flow(s). A-PCEF also translates PCC-R3 rule parameters into WiMAX SF Info parameters.
3. A-PCEF invokes the collocated Anchor SFA entity to initiate operation with WiMAX Service Flow(s). Anchor SFA sends *RR-Request* message to Serving SFA for Service Flow creation/ modification or deletion (including the requested SF Info parameters).
4. Serving SFA/ Anchor DP/ Acct Agent entity installs the policies and charging rules for the requested Service Flows. Note, that the activation of policies and charging rules occurs in step (8) when positive response is received from Serving BS. Otherwise, the newly installed policies are removed.
5. Anchor DP/ Serving SFA initiate data path operation corresponding to the requested Service Flow(s) operation – *Path Registration/ Modification/ Deregistration*.
6. Serving BS receives a request for data path/ Service Flow operation. If new radio resources allocation is requested, SFM entity, located in the BS, performs Admission Control operation.
7. If the request is admitted, Serving BS proceeds with Service Flow operation over-the-air using *DSx* transaction.

PCC

8. Serving BS responds to data path operation request with *Path Registration/ Modification/ Deregistration Rsp* message including the result of admission control and/ or over-the-air operation.
 9. Serving SFA sends *RR-Response* message to Anchor SFA providing the results for the requested operations with Service Flow(s).
 10. Anchor SFA invokes the collocated A-PCEF entity and the latter sends acknowledge to PDF/ PCRF for PCC rule provisioning request.
- Note that Acct Update is not presented on this flow.

E.3.2 A-PCEF initiated

Figure 29 presents intra-ASN message flow for MS-initiated request for bearer manipulation (Service Flow creation/ modification/ deletion) resulting in A-PCEF initiated (from PCC-R3 perspective) IP-CAN session modification.

This flow corresponds to the PCC-R3 message flow described in the Section 8.4.3.

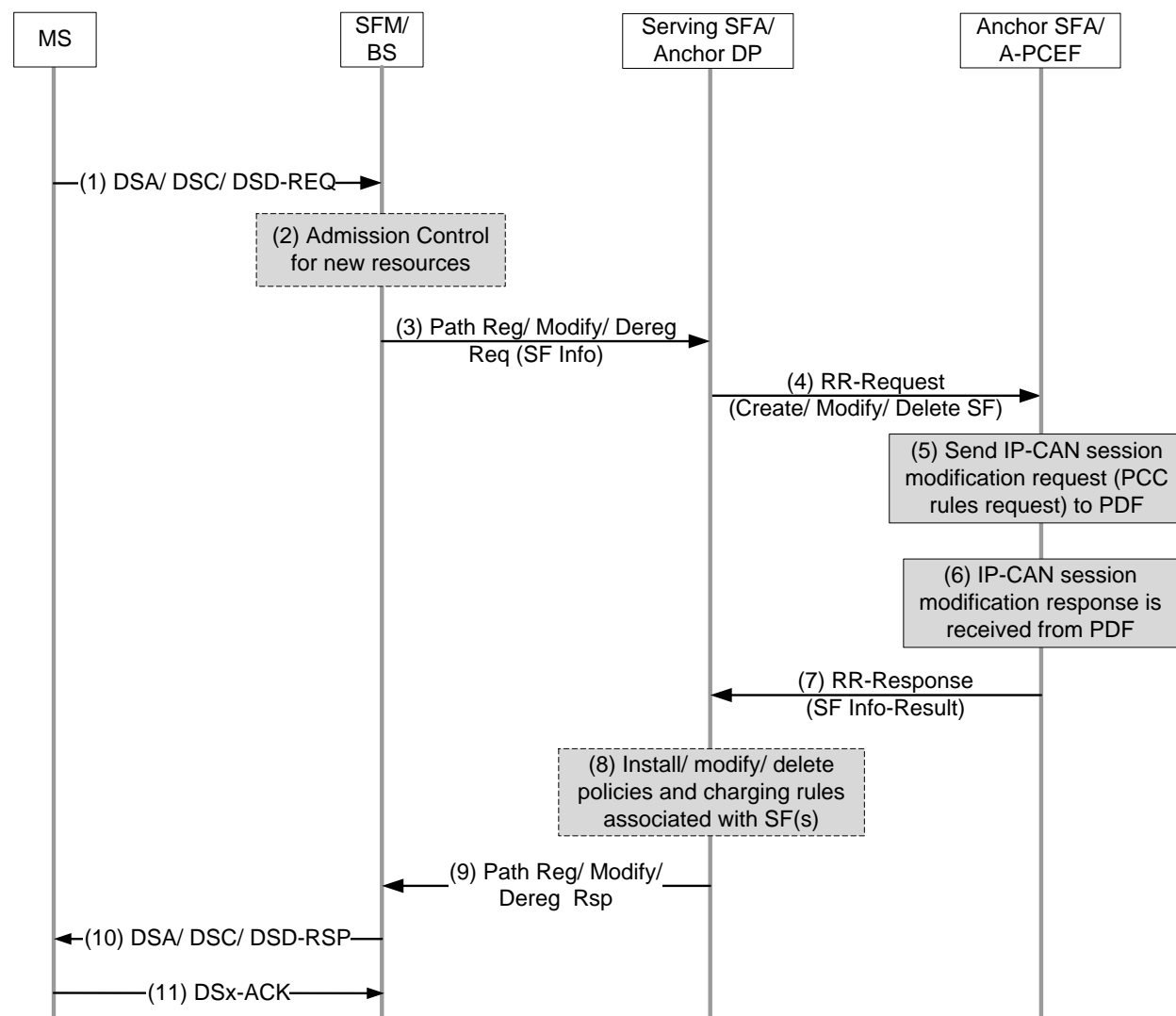


Figure 29: ASN procedures for MS initiated IP-CAN session modification

1. MS initiates operation with Service Flow – creation of a new Service Flow or modification/ deletion of one of the existing Service Flow(s). MS sends DSx-REQ message for this.

PCC

2. In the case new over-the-air resources are requested, BS/ SFM performs Admission Control decision.
 3. If the MS' request is admitted, BS starts the corresponding data path procedure – sends *Path Registration, Modification or Deregistration* message towards the MS' Anchor DP along the ASN data path. BS sets SF Info parameters to the values requested by MS in DSx-REQ (in the case of SF deletion, it is only SFID present in SF Info).
 4. Anchor DP invokes the collocated Serving SFA and the latter sends *RR-Request* message to Anchor SFA entity including the requested SF Info.
 5. Anchor SFA invokes A-PCEF entity. If multiple IP-CAN sessions are established for the MS, A-PCEF may need to identify the specific IP-CAN session, which is impacted by this MS request. A-PCEF sends IP-CAN session modification indication to PDF/ PCRF requesting authorization and PCC rule(s) for the bearer establishment/ modification (bearer termination may not require authorization). A-PCEF includes the requested bearer (Service Flow) parameters in this message.
 6. PDF/ PCRF acknowledge the request from A-PCEF and if the request is authorized, may provide PCC rule(s) for the required bearer.
 7. A-PCEF/ Anchor SFA sends *RR-Response* message to Serving SFA indicating the authorization decision and optionally the authorized parameters.
 8. If PCRF authorizes the request and provides new policies (or authorization parameters), Serving SFA/ Anchor DP install/ modify or delete policies/ charging rules associated with the requested Service Flow according to Anchor SFA instructions.
 9. Anchor DP sends *Path Registration/ Modification/ Deregistration* response to Serving BS along the ASN data path (indicating the authorization decision and optionally the authorized parameters).
 10. Serving BS updates admitted/ activated QoS according to authorized parameters (for SF establishment/ modification) and responds to MS with DSx-RSP message.
 11. MS acknowledges the DSx transaction completion by DSx-ACK message.
- Note that Acct Update is not presented on this flow.

E.3.3 BS-initiated bearer termination

Figure 30 presents intra-ASN message flow for BS-initiated Service Flow termination resulting in A-PCEF initiated IP-CAN session modification. Note that if multiple IP sessions are established for the MS and make use of the same bearer, then all the corresponding IP-CAN sessions are impacted.

This flow corresponds to the PCC-R3 message flow described in the Section 8.4.3.

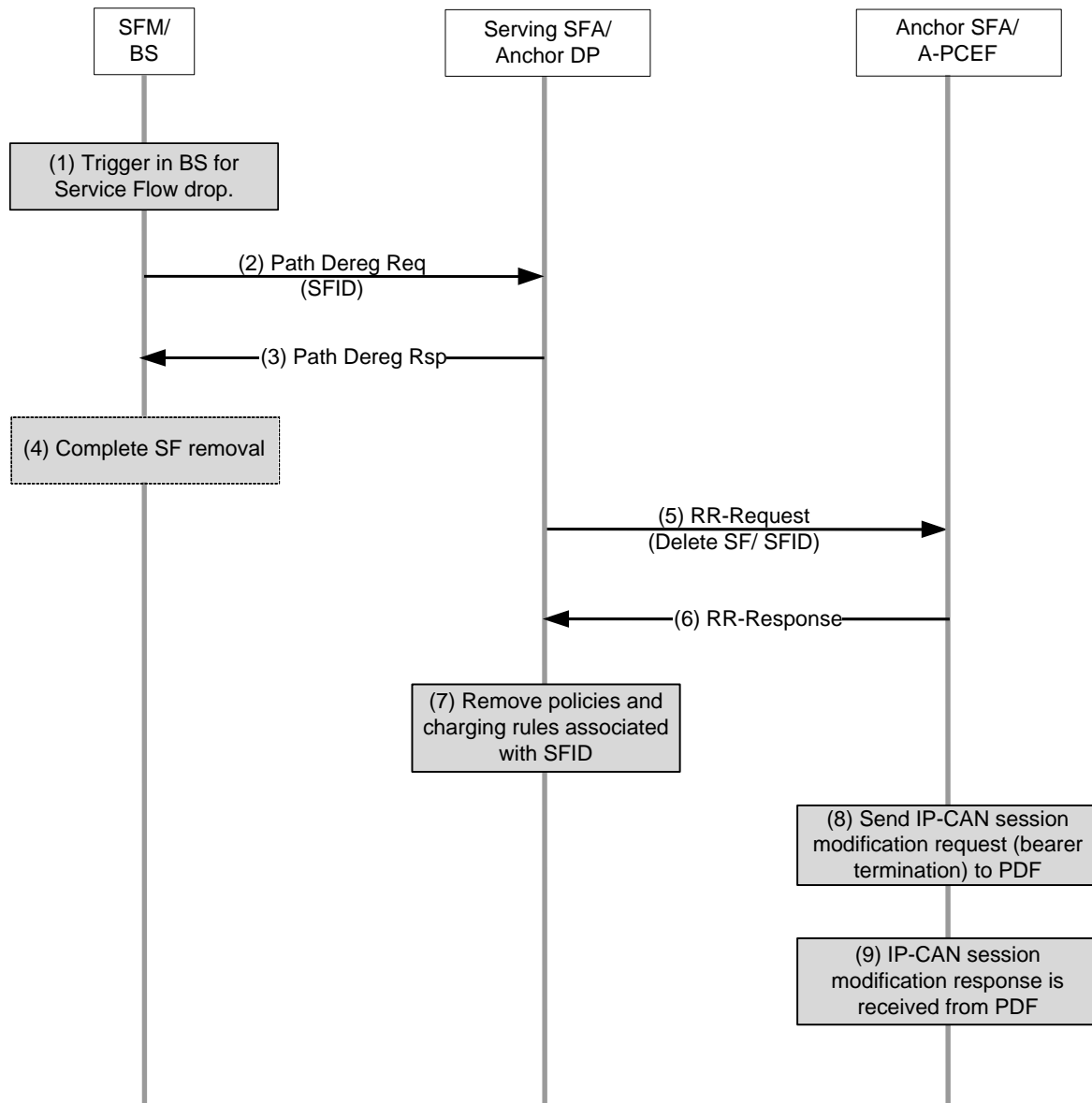


Figure 30: ASN procedures for BS initiated bearer termination

1. BS decides to drop MS' Service Flow e.g. as a part of changing radio conditions, etc. It is implementation decision whether BS performs over-the-air Service Flow termination immediately (DSD transaction or e.g. as a part of HO) or waits for Anchor SFA/ PCRF decision. As one of the options, BS may immediately proceed with DSD transaction (not presented on the flow). Note that signaling of Service Flow termination in HO may be implicit – e.g. by not confirming a new CID for the Service Flow (in BS RNG-RSP message).
2. BS sends *Path Deregistration Req* message for the corresponding Service Flow to Anchor DP along the ASN data path. Note that in the HO scenario this step is optional – BS does not perform Path Registration transaction for the terminated Service Flow. When Anchor DP/ Serving SFA Function detects that the data path for the specific Service Flow is not reestablished during HO, it triggers Service Flow termination procedure as described in this message flow starting from step 5.
3. Anchor DP responds with *Path Deregistration Rsp* message to BS along the ASN data path.

PCC

4. If BS has not performed over-the-air operation in step (1), then it initiates DSD transaction with MS for Service Flow termination.
 5. Same as step 4 of Figure 29.
 6. Same as step 7 of Figure 29.
 7. Serving SFA/ Anchor DP remove policies and charging rules associated with the impacted Service Flow.
 - 8-9. Same as steps 5-6 of Figure 29.
- Note that Acct Update is not presented on this flow.

E. 4 Handling mobility

E.4.1 A-PCEF relocation

Figure 31 presents intra-ASN message flow for A-PCEF relocation, which corresponds to the PCC-R3 message flow described in the Section 8.5.1.

A-PCEF is synonymous to Anchor SFA and is a functional entity instantiated in the ASN per MS (anchored per MS) and is collocated with MS' Anchored Authenticator and other per-MS anchored ASN functional entities – such as AAA Client and PMIP Client. A-PCEF relocation occurs as a result of Authenticator and AAA Client relocation when MS re-authentication process has been successfully completed in the ASN entity different from the previous MS' Anchored Authenticator.

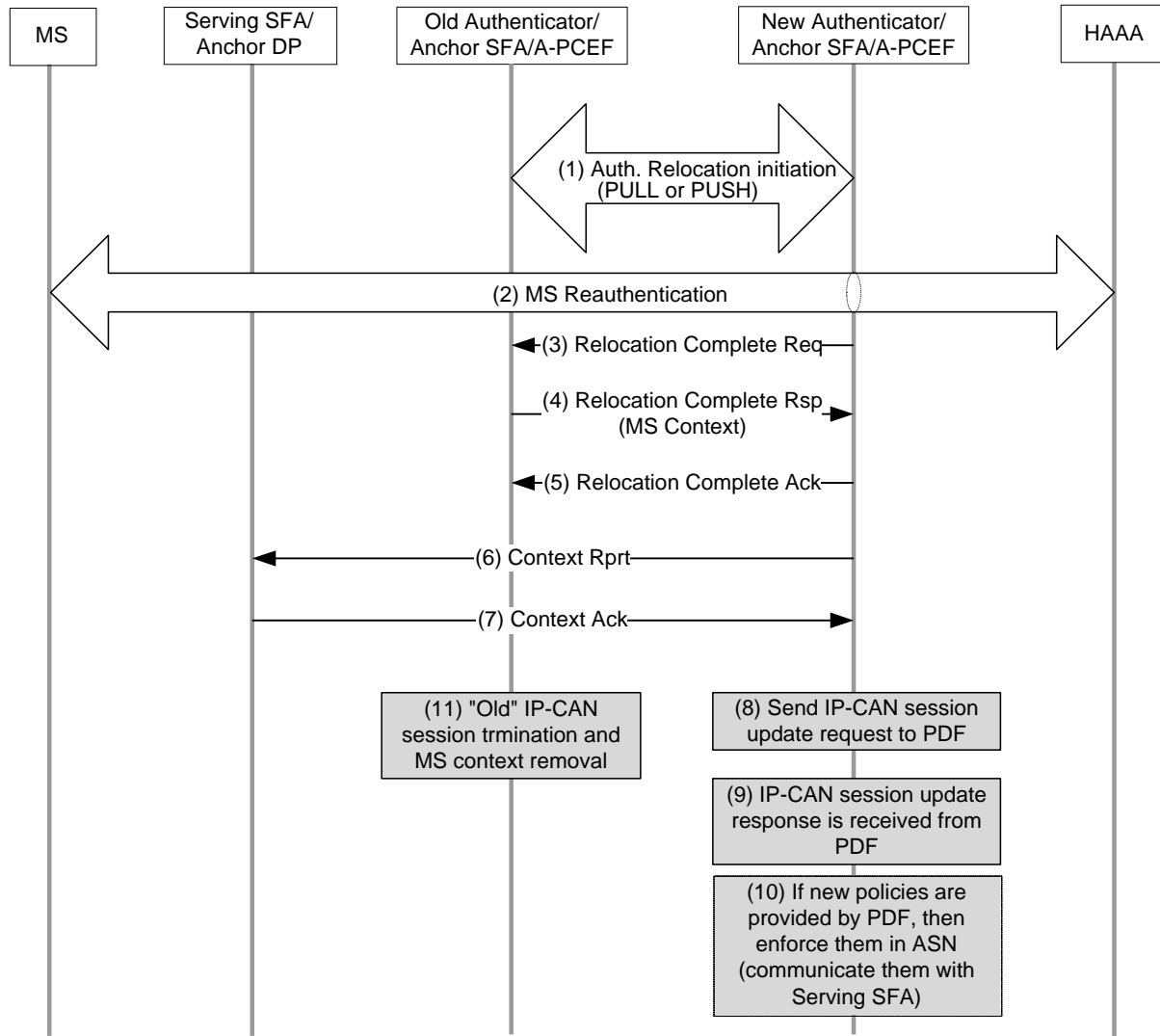


Figure 31: ASN procedures for A-PCEF relocation

1. Authenticator relocation PULL or PUSH interaction occurs between the “old” MS’ Anchored Authenticator and the “new” ASN entity starting MS reauthentication (“new” Authenticator). Part of MS context (e.g. MS Security History) is delivered to the “new” Authenticator in this transaction.
2. The “new” Authenticator initiates EAP-based reauthentication process. Supplicant in MS and Authentication Server in Home AAA perform EAP Authentication Method via the “new” Authenticator. Following the successful completion of EAP method, the “new” Authenticator forces key change procedure over the air (PKMv2 3-way handshake between the BS and the MS).
3. Once the “new” Authenticator detects successful completion of reauthentication process (Serving BS updates the “new” Authenticator that new security keys are successfully enforced over the air – successful PKMv2 3-way handshake completion), it sends Relocation Complete Req message to the “old” Authenticator. The “new” Authenticator requests delivery of the relevant MS context from the “old” Authenticator by setting proper bitmap in the Context Purpose Indicator TLV of this message.
4. The “old” Authenticator responds with Relocation Complete Rsp message including the requested MS context. This MS Context includes active PCC rules and their mapping into WiMAX Service Flows/ associated SF parameters.

PCC

- 1 5. The “new” Authenticator confirms the reception of Relocation Complete Rsp message by sending
2 Relocation Complete Ack.
 - 3 6. The “new” Authenticator/ Anchor SFA sends Context Report message to the Serving SFA/ Anchor DP
4 entity to update it about Authenticator relocation completion.
 - 5 7. The Serving SFA/ Anchor DP confirms reception of Context Rpt message by Context Ack.
 - 6 8. A-PCEF entity collocated with the “new” Authenticator initiates IP-CAN session update with PDF/ PCRF.
 - 7 9. PDF/ PCRF confirm IP-CAN session update and optionally may include new PCC rules in the response
8 message.
 - 9 10. If PDF/ PCRF provides new policies in the previous step, the “new” A-PCEF/ Anchor SFA should perform
10 “bearer binding” operation and then communicate WiMAX Service Flow changes (See section E.3.1) with
11 other ASN entities– Serving SFA and SFM over R4/ R6. Note that this operation is subject to admission
12 control decision in BS/ SFM if allocation of new resources is required and may be rejected by BS.
 - 13 11. “Old” A-PCEF proceeds with IP-CAN session termination (the leg between the “old” A-PCEF and PDF)
14 and MS context removal. For Radius-based PCC-R3 this step may occur immediately after the end of
15 Relocation Complete transaction. In the case of Diameter PCC-R3, termination of the “old” IP-CAN
16 session will be explicitly communicated between the “old” A-PCEF and PDF.
 - 17 Note that Acct Update is not presented on this flow.
-

18

19

Annex F Examples for Error Handling

Note: detailed messages are subject to change.

F.1 Type I Failure

Figure 32 shows two possible cases of type I failure which are due to network disconnection between A-PCEF and PDF/PCRF. On the A-PCEF side, a failure happens during IP-CAN session termination procedure. On the PDF/PCRF side, a failure happens during IP-CAN session modification procedure (i.e., removing the existing dynamic service flows).

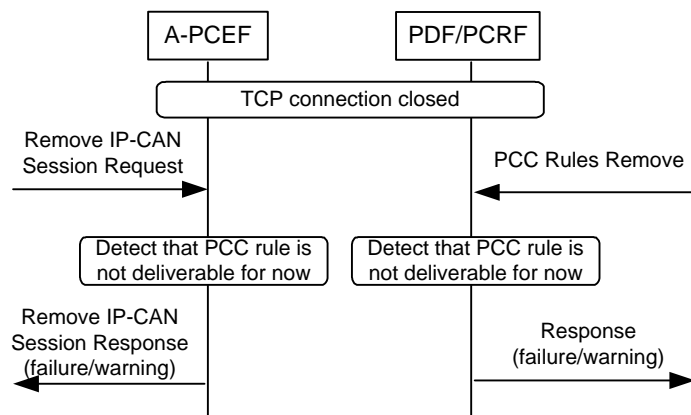


Figure 32: Example of Type I Failure

F.2 Type II Failure

Figure 33 shows an error case of type II failure which is due to delayed response. This figure is applicable when the successful response is delayed for an IP-CAN session modification (i.e., creating dynamic service flows).

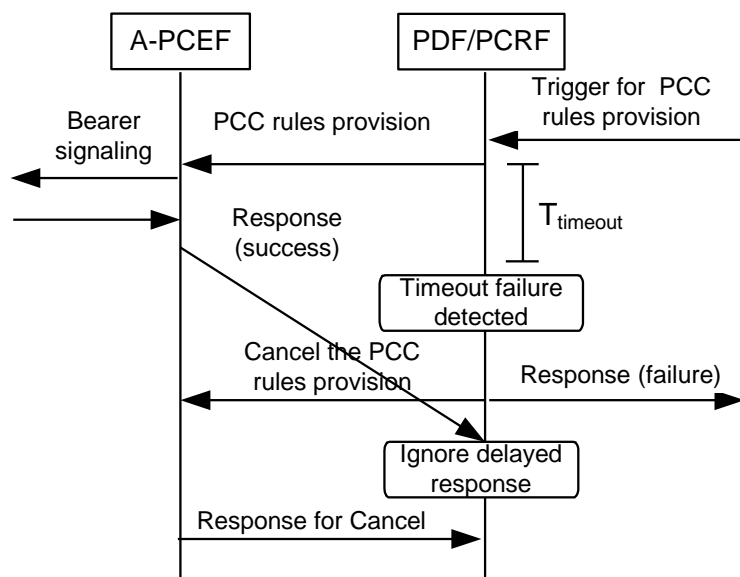


Figure 33: Example of Type II Failure

F. 3 Type III Failure

Figure 34 shows an error case of type III failure which is due to a response with failure result. This scenario is applicable when PDF/PCRF detects that PCC is not applicable (or allowed) for the MS during IP-CAN session establishment.

Note that possible values for Result-Code or Experimental-Result in CCA are defined in section 10.1.>

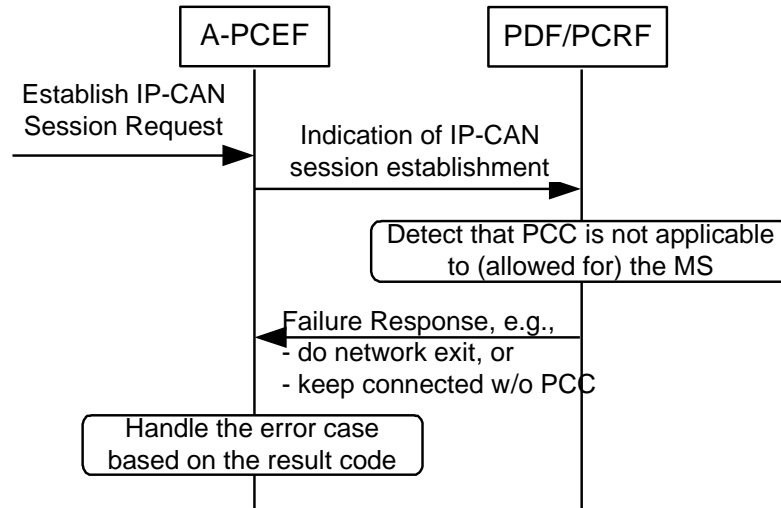


Figure 34 : Example of Type III Failure (Session Establishment Failure)

Figure 35 shows another error case of type III failure which is due to failure of PCC rules enforcement. This scenario can happen when the PCEF cannot install, delete or enforce rules from the PCRF. Detailed message parameters of RAR and RAA in this failure scenario can be found in [3].

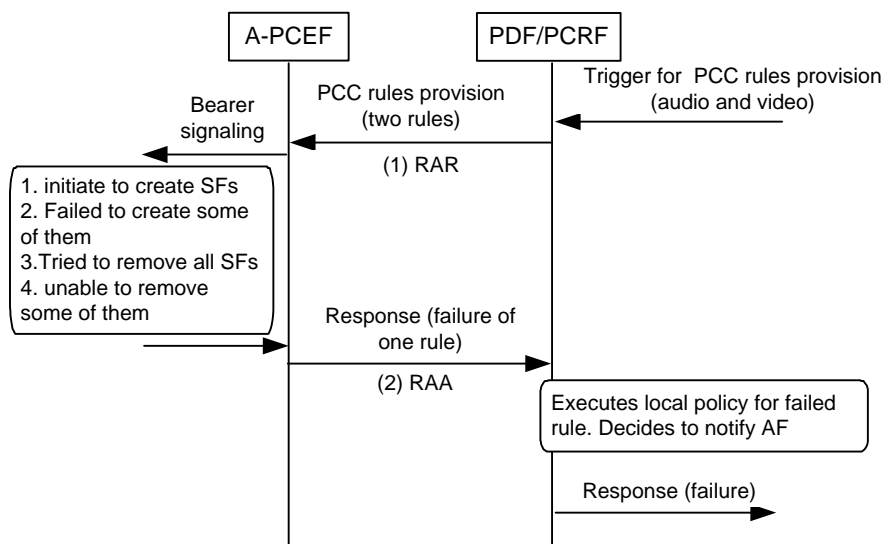


Figure 35 : Example of Type III Failure (PCC Rule Failure)

F. 4 The Error Handling During the IP-CAN Session Establishment

Figure 36 shows an error handling of IP-CAN session establishment where A-PCEF either initiates the network exit of MS or maintains ISF/PPSF without IP-CAN session establishment procedure according to local policy.

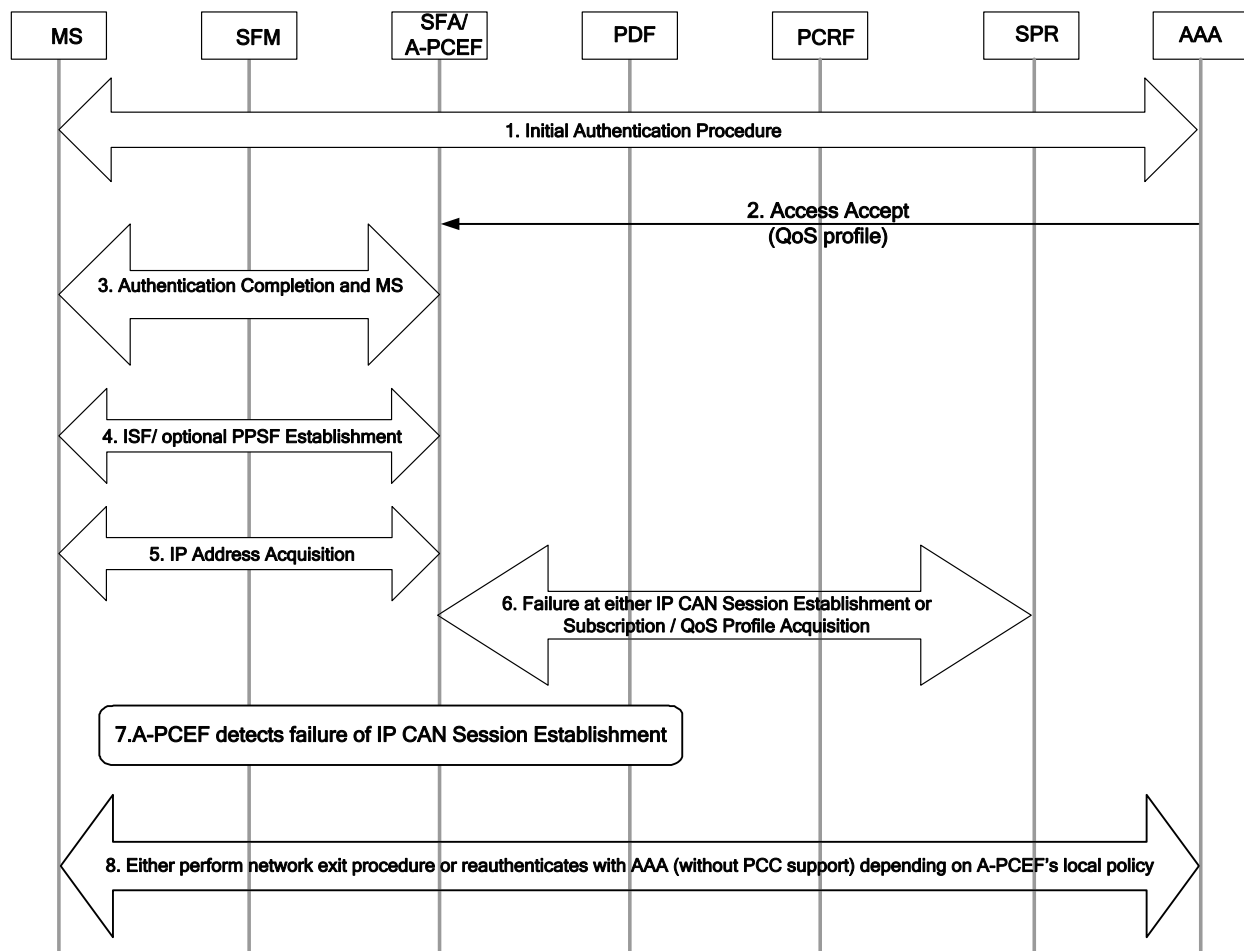


Figure 36 : Example for the error handling of IP CAN session establishment with network exit

1~5 The steps from 1 to 5 are correspondent to those of the Pre-provisioned service flow creation procedure described in section 8.1.1. Initial Service flow and pre-provisioned service flow creation.

6~7 If A-PCEF receives failure of Acknowledge IP-CAN session establishment or does not receive any Acknowledge message, it treats it as a failure case.(e.g. A-PCEF may initiates either network exit procedure or ISF/PPSF modification procedure according to the local policy of A-PCEF.)

8 If the local policy of A-PCEF for the failure of IP-CAN session establishment is the network exit for the failure of IP-CAN session establishment, A-PCEF triggers network exit procedure for ISF/PPSF. Or, if the local policy of A-PCEF for the failure of IP-CAN session establishment ISF/PPSF is to provide service without PCC, the A-PCEF/SFA SHALL trigger reauthentication procedure with the AAA authorize only, and set the WiMAX Capability AVP with PCC support removed. If the AAA authorizes service to the MS without PCC by returning an Access Accept, the session continues without PCC. If the AAA returns an Access Reject, the A-PCEF/SFA SHALL trigger network exit procedures for ISF/PPSF.

Annex G An Example of states synchronization

Figure 37 depicts an example of solving states inconsistency.

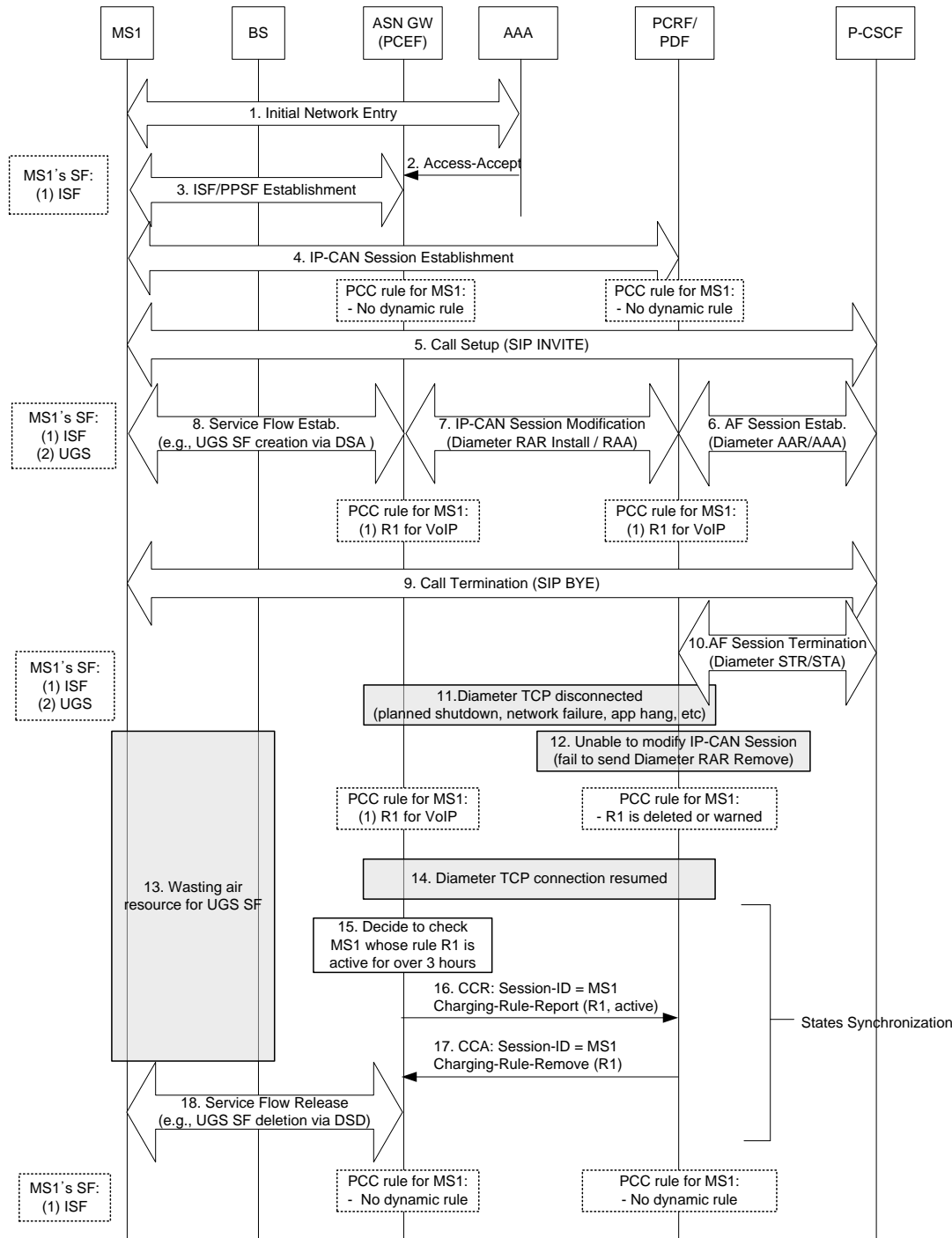


Figure 37 : Example of state synchronization

1~4 An IP-CAN session for MS1 is established.

PCC

- 1 5~8 While MS1 makes a call, dynamic service flows of UGS are created for the VoIP service. Both PCEF
2 and PDF/PCRF maintain the same PCC rule, R1.
- 3 9~13 The AF session (VoIP call session) has been terminated, but the PDF/PCRF is unable to trigger to
4 remove UGS service flows due to any reasons. So, failure of IP-CAN session modification happens
5 and this will make air resources wasted. The PCEF still maintain the PCC rule for VoIP but not at the
6 PDF/PCRF.
- 7 14~18 The PCEF finds that the PCC rule R1 needs to be reauthorized by PDF/PCRF. The PCEF sends CCR
8 message with the status of the PCC rule. Then, PDF/PCRF gets to know that PCEF keeps a rule that
9 has to be removed. So, the PDF/PCRF responds with a CCA message by including Charging-Rule-
10 Remove AVP for the rule. After this procedure, the PCEF and the PDF/PCRF maintain the same PCC
11 rule states.
- 12
- 13

