

Rx Interface Description

Ericsson Service-Aware Policy Controller

Interwork Description

Copyright

© Ericsson AB 2018. All rights reserved. No part of this document may be reproduced in any form without the written permission of the copyright owner.

Disclaimer

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Trademark List

All trademarks mentioned herein are the property of their respective owners. These are shown in the document [Trademark Information](#).



Contents

1	Rx Interface Overview	1
1.1	Document Content Conventions	1
2	Rx Interface Message Exchange	3
3	Diameter Base Protocol Messages	4
3.1	Rx Capability Negotiation	4
3.2	Device Watchdog	5
3.3	Disconnect Peer	6
4	Rx Interface Message Format	7
4.1	Rx AA-Request (AAR)	7
4.2	Rx AA-Answer (AAA)	9
4.3	Rx Re-Auth-Request (RAR)	10
4.4	Rx Re-Auth-Answer (RAA)	11
4.5	Rx Abort-Session-Request (ASR)	11
4.6	Rx Abort-Session-Answer (ASA)	12
4.7	Rx Session-Termination-Request (STR)	12
4.8	Rx Session-Termination-Answer (STA)	13
5	Rx Interface AVPS	14
5.1	Rx Supported-Features	14
5.2	Media-Component-Description AVP	16
5.3	Flow-Description AVP	17
6	Rx Error Handling	19
6.1	Rx Protocol Errors	19
6.2	Rx Application Errors	19
7	Reference List	23





1 Rx Interface Overview

This document describes the standard 3GPP Rx interface between an Application Function (AF) client and the SAPC.

3GPP Rx (*Policy and Charging Control over Rx reference point - 3GPP TS 29.214*) is built over Diameter Base Protocol RFC (*Diameter Base Protocol, IETF RFC 6733*). The SAPC supports 3GPP Rx from Rel9 onwards.

For detailed support about 3GPP Release versions of 3GPP Rx, refer to the corresponding Statement of Compliance documents.

1.1 Document Content Conventions

This document contains the specific details supported by the SAPC implementation.

This document does not repeat information that can be found in 3GPP Technical Specifications or Diameter Base Protocol RFC.

For detailed information about Statement of Compliance towards different 3GPP Release versions (for example Rel13, Rel14 and so on), see the corresponding SoCs documents.

Each message is described with the list of parameters (AVPs) exchanged between the Diameter peers.

- For **incoming** messages received in the SAPC, this document only indicates the AVPs that the SAPC reads to perform the corresponding business logic or evaluation inside policy conditions.

The SAPC can receive other AVPs (but does not use them) that can be found in 3GPP Technical Specifications, but are not stated in this document. This is possible because the SAPC uses a dictionary that specifies the format of messages and AVPs. The SAPC behaves in the following way (standard Diameter Base Protocol behavior):

1. If the SAPC receives in a message an AVP with M bit set to 1, and that AVP is not included in the dictionary, the SAPC rejects the message indicating DIAMETER_AVP_UNSUPPORTED.
2. If the SAPC receives in a message an AVP defined in the dictionary, but with different values in the flag bits, the SAPC rejects the message indicating DIAMETER_INVALID_AVP_BITS.
3. If the SAPC receives in a message an AVP with M bit set to 0, and that AVP is not defined in the dictionary, the SAPC does not reject the message, but ignores the AVP value.



- For **outgoing** messages (and AVPs) sent by the SAPC, this document indicates only the AVPs that the SAPC fills.

Note: When the SAPC does not support a message or AVP for all 3GPP Release versions, it is explicitly indicated in this document.



2 Rx Interface Message Exchange

As an example of the Diameter message exchange in a communication between an AF and the SAPC see next figure:

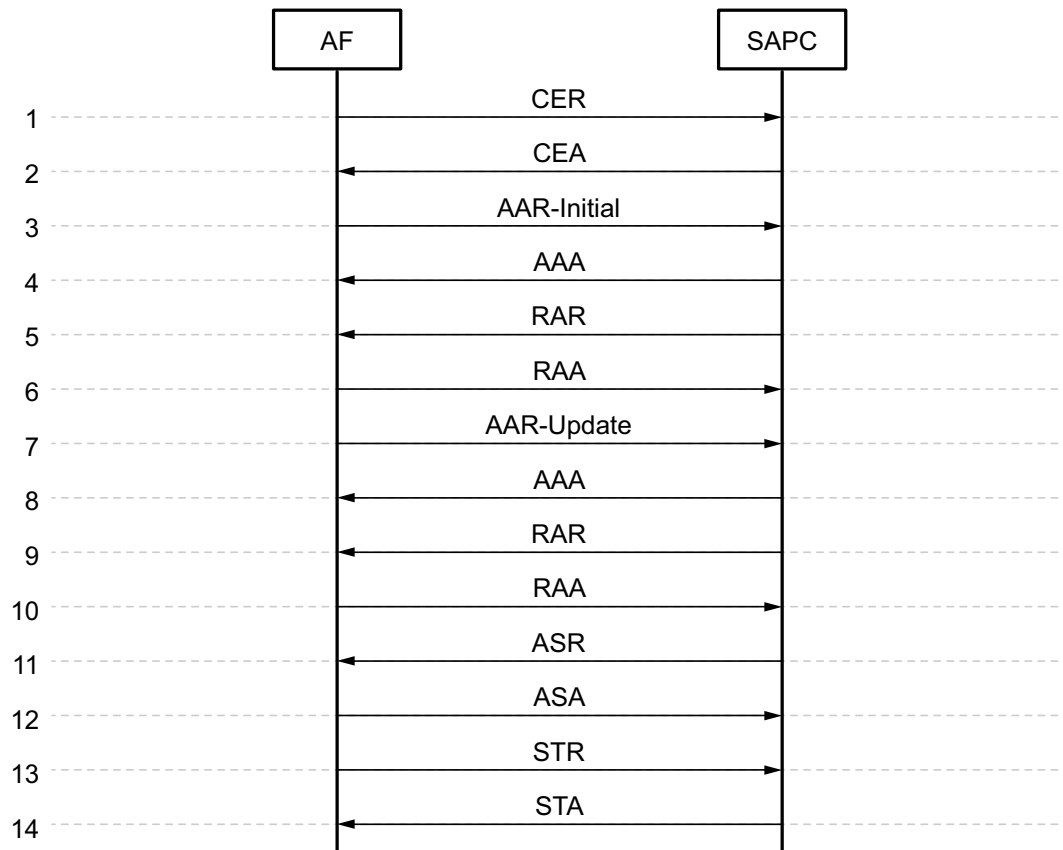


Figure 1 Rx Interface Message Flow



3 Diameter Base Protocol Messages

3.1 Rx Capability Negotiation

Next table lists the AVPs that the SAPC supports in a CER.

Table 1 CER AVPs

AVP Name	AVP Code	Comment	Reference
* [Acct-Application-Id]	259	-	RFC 6733
* [Auth-Application-Id]	258	-	RFC 6733
[Firmware-Revision]	367	-	RFC 6733
1* { Host-IP-Address }	257	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
{ Product-Name }	269	-	RFC 6733
* [Supported-Vendor-Id]	265	-	RFC 6733
{ Vendor-Id }	266	-	RFC 6733
*[Vendor-Specific-Application-Id]	260	-	RFC 6733

[Table 2](#) lists the AVPs that the SAPC sends in a CEA message.

Table 2 CEA AVPs

AVP Name	AVP Code	Comment	Reference
{Auth-Application-Id}	258	-	RFC 6733
[Error-Message]	281	-	RFC 6733
[Failed-AVP]	279	-	RFC 6733
[Firmware-Revision]	367	-	RFC 6733
1*{Host-IP-Address}	257	-	RFC 6733
{Origin-Host}	264	-	RFC 6733



AVP Name	AVP Code	Comment	Reference
{Origin-Realm}	296	-	RFC 6733
[Product-Name]	269	-	RFC 6733
[Result-Code]	268	-	RFC 6733
*[Supported-Vendor-Id]	265	According to configuration, the SAPC sends the values assigned to other supported vendors different than the vendor device (Ericsson): —10415 (3GPP) —13019 (ETSI). Supported for Rel10 onwards	RFC 6733
Vendor-Id	266	The SAPC sets it to value 193 (Ericsson).	RFC 6733
*[Vendor-Specific-Application-Id]	260	According to configuration, the SAPC sends the following AVP values: —Vendor-Id= 10415 (3GPP) —Auth-Application-Id= 16777236 (3GPP Rx)	RFC 6733

Note: The SAPC does not sent Origin-State-Id AVP in CEA message.

3.2 Device Watchdog

[Table 3](#) lists the AVPs that the SAPC can receive or send in a DWR message.

Table 3 DWR AVPs

AVP Name	AVP Code	Comment	Reference
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
[Origin-State-Id]	278	-	RFC 6733

Note: The SAPC does not include Origin-State-Id AVP when it sends an outgoing DWR message.

[Table 4](#) lists the AVPs that the SAPC can receive or send in a DWA message.



Table 4 DWA AVPs

AVP Name	AVP Code	Comment	Reference
[Error-Message]	281	-	RFC 6733
[Failed-AVP]	279	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
[Origin-State-Id]	278	-	RFC 6733

Note: The SAPC does not include Origin-State-Id AVP when it sends an outgoing DWA message.

3.3 Disconnect Peer

[Table 5](#) lists the AVPs that the SAPC supports in a DPR message.

Table 5 DPR AVPs

AVP Name	AVP Code	Comment	Reference
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
{ Disconnect-Cause }	273	-	RFC 6733

[Table 6](#) lists the AVPs that the SAPC supports in a DPA message.

Table 6 DPA AVPs

AVP Name	AVP Code	Comment	Reference
[Error-Message]	281	-	RFC 6733
[Failed-AVP]	279	-	RFC 6733
{ Origin-Host }	264	-	RFC 6733
{ Origin-Realm }	296	-	RFC 6733
{ Result-Code }	268	-	RFC 6733



4 Rx Interface Message Format

For Rx Interface commands Auth-Application-Id AVP is set to 16777236.

4.1 Rx AA-Request (AAR)

[Table 7](#) lists the AVPs that the SAPC supports in an AAR.

Table 7 AAR AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
[AF-Application-Identifier]	504	-	3GPP TS 29.214
[AF-Charging-Identifier]	505	-	3GPP TS 29.214
{Auth-Application-Id}	258	-	3GPP TS 29.214
[Called-Station-Id]	30	-	See RFC 4005
[Destination-Host]	293	-	RFC 6733
{Destination-Realm}	283	-	RFC 6733
[Framed-IP-Address] ⁽¹⁾	8	-	RFC 4005
[Framed-IPv6-Prefix] ⁽¹⁾	97	-	RFC 4005
[IP-Domain-Id]	537	-	3GPP TS 29.214
*[Media-Component-Description]	518	See Media-Component-Description AVP on page 16.	3GPP TS 29.214
[MPS-Identifier]	528	Supported for Rel10 onwards.	3GPP TS 29.214
{Origin-Host}	264	-	RFC 6733
{Origin-Realm}	296	-	RFC 6733
[Origin-State-Id]	278	-	RFC 6733
*[Required-Access-Info]	536	-	3GPP TS 29.214



AVP Name	AVP Code	Comment	Reference
[Reservation-Priority]	458	-	ETSI TS 183.017
[Rx-Request-Type]	533	The SAPC supports the following values: —INITIAL_REQUEST (0) —UPDATE_REQUEST (1) —PCSCF_RESTORATION (2) ⁽²⁾	3GPP TS 29.214
[Service-Info-Status]	527	-	3GPP TS 29.214
[Service-URN]	525	-	3GPP TS 29.214
*[Specific-Action]	513	The SAPC supports the following values: —INDICATION_OF_RELEASE_OF_BEARER (4) —IP-CAN_CHANGE (6) —INDICATION_OF_SUCCESSFUL_RESOURCES_ALLOCATION (8) —INDICATION_OF_FAILED_RESOURCES_ALLOCATION (9) —ACCESS_NETWORK_INFO_REPORT (12)	3GPP TS 29.214
[SIP-Forking-Indication]	523	The SAPC uses the default value SINGLE_DIALOGUE (0), when this AVP is omitted.	3GPP TS 29.214
*[Subscription-Id]	443	If the SAPC receives several instances of this AVP, it uses: —The value contained in Subscription-Id-Data of the first Subscription-Id AVP received —Or the value contained in Subscription-Id-Data corresponding to the Subscription-Id-Type set in a configurable parameter in the SAPC.	RFC 4006
*[Supported-Features]	628	See Rx Supported-Features on page 14.	3GPP TS 29.229

(1) Framed-IP-Address or Framed-IPv6-Prefix AVPs are mandatory to be received for the SAPC in AAR-Initial. Otherwise, the SAPC returns Result-Code AVP set to DIAMETER_MISSING_AVP.



- (2) If the SAPC receives PCSCF_RESTORE (2) it returns Result-Code AVP set to DIAMETER_INVALID_AVP_VALUE.

4.2 Rx AA-Answer (AAA)

[Table 8](#) lists the AVPs that the SAPC sends in an AAA.

Table 8 AAA AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
[AN-Trusted]	1503	-	3GPP TS 29.273
{Auth-Application-Id}	258	-	3GPP TS 29.214
[Experimental-Result-Code]	298	See Table 18	3GPP TS 29.214
[Failed-AVP]	279	-	RFC 6733
[IP-CAN-Type]	1027	See values listed in Gx Interface Description.	3GPP TS 29.212
[NetLoc-Access-Support]	2824	The SAPC sends it when the AF requested NetLoc, but the PCEF does not support NetLoc. The SAPC supports the following values: —NETLOC_ACCESS_NOT_SUPPORTED (0)	3GPP TS 29.212
{Origin-Host}	264	-	RFC 6733
{Origin-Realm}	296	-	RFC 6733
[Origin-State-Id]	278	The SAPC increments its value in standalone mode after restart. In geographical redundancy, the SAPC does not increment its value unless both SAPC peers are down. This MUST never happen, as the SAPC does a transparent switch-over (the Diameter peer always sees an operative node, the one in active state).	RFC 6733
[RAT-Type]	1032	-	3GPP TS 29.212
[Result-Code]	268	-	RFC 6733
*[Supported-Features]	628	See Rx Supported-Features on page 14.	3GPP TS 29.229



4.3 Rx Re-Auth-Request (RAR)

Table 9 lists the AVPs that the SAPC sends in a RAR.

Table 9 RAR AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
[3GPP-MS-TimeZone]	23	(1)	3GPP TS 29.061
[3GPP-SGSN-MCC-MNC]	18	(1)	3GPP TS 29.061
[3GPP-User-Location-Info]	22	(1)	3GPP TS 29.061
[Abort-Cause]	500	The SAPC supports the following values: —BEARER_RELEASED (0) —PS_TO_CS_HANDOVER (3).	3GPP TS 29.214
[AN-Trusted]	1503	-	3GPP TS 29.273
{Auth-Application-Id}	258	-	3GPP TS 29.214
{Destination-Host}	293	-	RFC 6733
{Destination-Realm}	283	-	RFC 6733
[Flows]	510	The SAPC supports the following AVPs: —{ Media-Component-Number } —[Flow-Number]	3GPP TS 29.214
[IP-CAN-Type]	1027	See values listed in Gx Interface Description.	3GPP TS 29.212
[NetLoc-Access-Support]	2824	The SAPC sends it when the AF requested NetLoc, but the PCEF or the IP-CAN session do not support NetLoc, or when the AF requested NetLoc, and the PCEF sends NetLoc information for untrusted WLAN, but the AF does not support NetLoc-Untrusted-WLAN The SAPC supports the following values: —NETLOC_ACCESS_NOT_SUPPORTED (0)	3GPP TS 29.212
{Origin-Host}	264	-	RFC 6733



AVP Name	AVP Code	Comment	Reference
{Origin-Realm}	296	-	RFC 6733
[Origin-State-Id]	278	The SAPC increments its value in standalone mode after restart. In geographical redundancy, the SAPC does not increment its value unless both peers are down. This MUST never happen, as the SAPC does a transparent switch-over (the Diameter peer always sees an operative node, the one in active state).	RFC 6733
[RAT-Type]	1032	-	3GPP TS 29.212
*{Specific-Action}	513	Besides the values listed in *[Specific-Action] in Table 7 , the SAPC supports the following values: —INDICATION_OF_ACCESS_NETWORK_INFO_REPORTING_FAILURE (14)	3GPP TS 29.214
[User-Location-Info-Time]	2812	(1)	3GPP TS 29.212
[TWAN-Identifier]	29	(2)	3GPP TS 29.061
[UE-Local-IP-Address]	2805	(2)	3GPP TS 29.212
[TCP-Source-Port]	2843	(2)	3GPP TS 29.212
[UDP-Source-Port]	2806	(2)	3GPP TS 29.212
0*2[AN-GW-Address]	1050	-	3GPP TS 29.212

(1) The SAPC sends this AVP if the AF requested NetLoc, and if the SAPC received this AVP from the PCEF.

(2) The SAPC sends this AVP if the AF requested NetLoc, and if the SAPC received this AVP from the PCEF and if the AF supports NetLoc-Untrusted-WLAN.

4.4 Rx Re-Auth-Answer (RAA)

The SAPC does not read any AVPs received in RAA answers, except Session-Id AVP and Result-Code AVP.

4.5 Rx Abort-Session-Request (ASR)

[Table 10](#) lists the AVPs that the SAPC sends in an ASR.



Table 10 ASR AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
[Abort-Cause]	500	The SAPC supports the following values: —BEARER_RELEASED (0) —PS_TO_CS_HANDOVER (3).	3GPP TS 29.214
{Auth-Application-Id}	258	-	3GPP TS 29.214
{Destination-Host}	293	-	RFC 6733
{Destination-Realm}	283	-	RFC 6733
{Origin-Host}	264	-	RFC 6733
{Origin-Realm}	296	-	RFC 6733
[Origin-State-Id]	278	The SAPC increments its value in standalone mode after restart. In geographical redundancy, the SAPC does not increment its value unless both peers are down. This MUST never happen, as the SAPC does a transparent switch-over (the Diameter peer always sees an operative node, the one in active state).	RFC 6733

4.6 Rx Abort-Session-Answer (ASA)

The SAPC does not read any AVPs received in ASA answers, except Session-Id AVP and Result-Code AVP.

4.7 Rx Session-Termination-Request (STR)

[Table 11](#) lists the AVPs that the SAPC supports in a STR.

Table 11 STR AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
*[Required-Access-Info]	536	-	3GPP TS 29.214



4.8 Rx Session-Termination-Answer (STA)

Table 12 lists the AVPs that the SAPC sends in an STA.

Table 12 STA AVPs

AVP Name	AVP Code	Comment	Reference
<Session-Id>	263	-	RFC 6733
[3GPP-MS-TimeZone]	23	(1)	3GPP TS 29.061
[3GPP-SGSN-MCC-MNC]	18	(1)	3GPP TS 29.061
[3GPP-User-Location-Info]	22	(1)	3GPP TS 29.061
[Failed-AVP]	279	-	RFC 6733
[NetLoc-Access-Support]	2824	The SAPC sends it when the AF requested NetLoc, but the PCEF or the IP-CAN session do not support NetLoc, or when the AF requested NetLoc, and the PCEF sends NetLoc information for untrusted WLAN, but the AF does not support NetLoc-Untrusted-WLAN The SAPC supports the following values: —NETLOC_ACCESS_NOT_SUPPORTED (0)	3GPP TS 29.212
{Origin-Host}	264	-	RFC 6733
{Origin-Realm}	296	-	RFC 6733
[Origin-State-Id]	278	-	RFC 6733
[Result-Code]	268	-	RFC 6733
[User-Location-Info-Time]	2812	(1)	3GPP TS 29.212
[TWAN-Identifier]	29	(2)	3GPP TS 29.061
[UE-Local-IP-Address]	2805	(2)	3GPP TS 29.212
[TCP-Source-Port]	2843	(2)	3GPP TS 29.212
[UDP-Source-Port]	2806	(2)	3GPP TS 29.212

(1) The SAPC sends this AVP if the AF requested NetLoc, and if the SAPC received this AVP from the PCEF.

(2) The SAPC sends this AVP if the AF requested NetLoc, and if the SAPC received this AVP from the PCEF and if the AF supports NetLoc-Untrusted-WLAN.



5 Rx Interface AVPS

The following subsections contain information for AVPs, that owing to space reasons, cannot be explained inside Message tables of [Rx Interface Message Format](#) on page 7.

5.1 Rx Supported-Features

Depending on the information received from the AF during session establishment in Feature-List AVP within Supported-Features AVP, the SAPC decides the particular Release feature used in Rx, according to [Table 13](#).

Note: The SAPC includes Supported-Features AVP only when Result-Code AVP value is 2001 (SUCCESS). The SAPC does not send Supported-Features AVP if Result-Code AVP value is different than 2001 (SUCCESS).

Note: The SAPC ignores the value of Supported-Features AVP during AF session modification, if present in the AAR command.

Table 13 Supported-Feature instance with Feature-List-ID 1

Feature	Received and Sent Features-List AVP bit Values, inside Supported-Features AVP with Feature-List-ID 1
NetLoc-Untrusted-WLAN	If the SAPC receives bit 16 = 1 in AAR command and the NetLoc function is enabled, the SAPC answers AAA including bit 16 = 1. It requires that the SAPC also receives bit 5 = 1.
NetLoc	If the SAPC receives bit 5 = 1 in AAR command and the NetLoc function is enabled, the SAPC answers AAA including bit 5 = 1.
ProvAFsignal Flow	If the SAPC receives bit 2 = 1 in AAR command and the dynamic policy control function is enabled, the SAPC answers AAA including bit 2 = 1.
Rx Rel10	<p>If the SAPC receives from the AF in AAR command:</p> <pre>Supported-Features { Vendor-Id = 10415 } { Feature-List-ID = 1 } { Feature-List bit 0 = x (any value) bit 1 = x (any value) bit 4 = 1 rest of bits = x (any value)}</pre> <p>the SAPC answers AAA including:</p>



Feature	Received and Sent Features-List AVP bit Values, inside Supported-Features AVP with Feature-List-ID 1
	Supported-Features { Vendor-Id = 10415 } { Feature-List-ID = 1 } { Feature-List bit 0 = x (same value than received in AAR) bit 1 = x (same value than received in AAR) bit 4 = 1 rest of bits = 0 }
Rx Rel9	If the SAPC receives from the AF in AAR command: Supported-Features { Vendor-Id = 10415 } { Feature-List-ID = 1 } { Feature-List bit 0 = x (any value) bit 1 = 1 bit 4 = 0 rest of bits = x (any value)} the SAPC answers AAA including: Supported-Features { Vendor-Id = 10415 } { Feature-List-ID = 1 } { Feature-List bit 0 = x (same value than received in AAR) bit 1 = 1 bit 4 = 0 rest of bits = 0 }
Rx Rel8	If the SAPC receives from the AF in AAR command: Supported-Features { Vendor-Id = 10415 } { Feature-List-ID = 1 } { Feature-List bit 0 = 1 bit 1 = 0 bit 4 = 0 rest of bits = x (any value)} the SAPC answers AAA with Result-Code AVP set to DIAMETER_INVALID_AVP_VALUE, and including Supported-Features AVP inside Failed-AVP AVP.
Rx Rel7	If the SAPC receives from the AF an AAR command without Supported-Features AVP, the SAPC responds AAA with Result-Code AVP set to DIAMETER_MISSING_AVP, including Supported-Features AVP inside Failed-AVP AVP.



Table 14 Supported-Features instance with Feature-List-ID 2

Feature	Received and Sent Features-List AVP bit Values, inside Supported-Features AVP with Feature-List-ID 2
Extended-Max-Requested-BW-NR	If the SAPC receives bit 1 = 1 in AAR command and the extend bit rates over Rx function is licensed, the SAPC answers AAA including bit 1 = 1.

5.2 Media-Component-Description AVP

Table 15 Media-Component-Description AVPs

AVP Name	AVP Code	Comment	Reference
[AF-Application-Identifier]	504	-	3GPP TS 29.214
[Extended-Max-Requested-BW-DL]	554	Downlink bandwidth information provided within the Media-Sub-Component AVP takes precedence over the value provided by this AVP.	3GPP TS 29.214
[Extended-Max-Requested-BW-UL]	555	Uplink bandwidth information provided within the Media-Sub-Component AVP takes precedence over the value provided by this AVP.	3GPP TS 29.214
[Flow-Status]	511	Flow status information provided within the Media-Sub-Component AVP takes precedence over the value provided by this AVP.	3GPP TS 29.214
[Max-Requested-Bandwidth-DL]	515	Downlink bandwidth information provided within the Media-Sub-Component AVP takes precedence over the value provided by this AVP.	3GPP TS 29.214
[Max-Requested-Bandwidth-UL]	516	Uplink bandwidth information provided within the Media-Sub-Component AVP takes precedence over the value provided by this AVP.	3GPP TS 29.214
{Media-Component-Number}	518	-	3GPP TS 29.214
*[Media-Sub-Component]	519	The SAPC supports the following AVPs within it: —{ Flow-Number }	3GPP TS 29.214



AVP Name	AVP Code	Comment	Reference
		—0*2[Flow-Description] —[Flow-Usage] —[Flow-Status] —[Max-Requested-Bandwidth-UL] —[Extended-Max-Requested-BW-UL] —[Max-Requested-Bandwidth-DL] —[Extended-Max-Requested-BW-DL] —[AF-Signalling-Protocol]	
[Media-Type]	520	-	3GPP TS 29.214
[Reservation-Priority]	458	-	ETSI TS 183.017
[RS-Bandwidth]	521	-	3GPP TS 29.214
[RR-Bandwidth]	522	-	3GPP TS 29.214

5.3 Flow-Description AVP

The Flow-Description AVP (AVP code 507) is of type *IPFilterRule*, and defines a packet filter for an IP flow with the following information:

- Direction (in or out). The direction "in" refers to uplink IP flows, and the direction "out" refers to downlink IP flows.
- Source and destination IP address (possibly masked)
- Protocol
- Source and destination port

The *IPFilterRule* type has to be used over Rx interface with the following restrictions:

- The Source Port can be omitted to indicate that any source port is allowed. Lists or ranges cannot be used. For TCP, destination port can also be omitted.
- Only the Action "permit" can be used.



- No "options" can be used.
- The invert modifier "!" for addresses cannot be used.
- The keyword "assigned" cannot be used.



6 Rx Error Handling

When the SAPC detects an error at protocol or application level, it returns a response including the `Result-Code` AVP with an error code specifying the error.

6.1 Rx Protocol Errors

The SAPC handles the following Diameter Base Protocol error types:

Table 16 SAPC Diameter Base Protocol Errors

Diameter Result Code	Value	Description
DIAMETER_SUCCESS	2001	A request is successfully completed.
DIAMETER_COMMAND_UNSUPPORTED	3001	A request contains a <code>Command-Code</code> that the SAPC does not recognize or support.
DIAMETER_TOO_BUSY	3004	A request is received when the SAPC is overloaded.
DIAMETER_APPLICATION_UNSUPPORTED	3007	A request is received for an unsupported application.
DIAMETER_INVALID_HDR_BITS	3008	A request is received with a Diameter header whose bits are set to an invalid combination or to a value that is inconsistent with the <code>Command-Code</code> definition.
DIAMETER_INVALID_AVP_BITS	3009	A request is received with an AVP whose flag bits are set to an unrecognized value or are inconsistent with the AVPs definition.
DIAMETER_UNKNOWN_PEER	3010	A CER message is received from an unknown peer.

6.2 Rx Application Errors

The SAPC handles the following Rx Interface Application errors:



Table 17 SAPC Application Errors

Diameter Result Code	Value	Description
DIAMETER_OUT_OF_SPACE	4002	A Diameter node received the request but was unable to commit it to stable storage due to a temporary lack of space.
ELECTION_LOST	4003	The peer has determined that it has lost the election process and has therefore disconnected the transport connection.
DIAMETER_AVP_UNSUPPORTED	5001	<p>A request is received with an AVP that is not recognized or supported (not included in the SAPC Diameter dictionary) and was marked with the Mandatory bit.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the AVPs that caused the failure.</p>
DIAMETER_UNKNOWN_SESSION_ID	5002	Returned if the session does not exist for the UE IP address at session modification/termination.
DIAMETER_INVALID_AVP_VALUE	5004	<p>A request is received with an AVP with an invalid value in its data portion.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the AVPs that caused the failure.</p>
DIAMETER_MISSING_AVP	5005	When a request is received including an AVP that is not required to process that request, that AVP is ignored and the request is processed as usual. On the contrary, when a request does not include an AVP that is required to process such request, the SAPC returns a response including Result-Code DIAMETER_MISSING_AVP and the Failed-AVP AVP.
DIAMETER_CONTRADICTING_AVPS	5007	<p>A request is received with AVPs that are contradicted each other.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the AVPs that caused the failure.</p>
DIAMETER_AVP_NOT_ALLOWED	5008	A request is received with an AVP that must not be present.



Diameter Result Code	Value	Description
		A Diameter message with this error must contain a Failed-AVP AVP with a copy of the offending AVP.
DIAMETER_AVP_OCCURS_TOO_MANY_TIMES	5009	<p>A request is received with an AVP that appears more often than permitted in the message definition.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP with a copy of the first instance of the offending AVP that exceeded the maximum number of occurrences.</p>
DIAMETER_NO_COMMON_APPLICATION	5010	A CER message is received and there are no common applications supported between the SAPC and the peer.
DIAMETER_UNSUPPORTED_VERSION	5011	A request is received with an unsupported version number.
DIAMETER_UNABLE_TO_COMPLY	5012	This error is returned when the SAPC receives a request and detects an internal error which does not allow to continue processing a request.
DIAMETER_INVALID_BIT_IN_HEADER	5013	A request is received with an unrecognized bit in the Diameter header is set to one.
DIAMETER_INVALID_AVP_LENGTH	5014	<p>A request is received containing an AVP with an invalid length.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the offending AVP.</p>
DIAMETER_INVALID_MESSAGE_LENGTH	5015	A request is received with an invalid message length.
DIAMETER_INVALID_AVP_BIT_COMBO	5016	<p>A request is received with an AVP which is not allowed to have the received value in the AVP Flags field.</p> <p>A Diameter message with this error must contain a Failed-AVP AVP containing the offending AVP.</p>
DIAMETER_NO_COMMON_SECURITY	5017	<p>This error is returned when a CER message is received, and there are no common security mechanisms supported between the peers.</p> <p>A CEA MUST be returned with the Result-Code AVP set to DIAMETER_NO_COMMON_SECURITY.</p>



The SAPC handles the following Rx Interface Application errors, using Experimental-Result-Code AVP (where Vendor-Id AVP is set to 10415):

Table 18 The SAPC Application Errors, Experimental Results

Experimental-Result-Code within Experimental-Result	Value	Description
REQUESTED_SERVICE_NOT_AUTHORIZED	5063	The SAPC rejects new or modified service information because the requested service, as described by the service information provided by the AF, is not consistent with either the related subscription information or operator defined policy rules.
IP-CAN_SESSION_NOT_AVAILABLE	5065	The SAPC rejects a new Rx session setup when it fails to perform session binding within the session information received from the AF to a unique existing IP-CAN session.
UNAUTHORIZED_NON_EMERGENCY_SESSION	5066	The SAPC rejects a new Rx session setup that binds to an emergency IP-CAN session and the Service-URN AVP is missing or does not contain a top-level service type of "sos"



7 Reference List

Standards references

1. Policy and Charging Control over Rx reference point - 3GPP TS 29.214
2. Cx and Dx interfaces based on Diameter protocol; Protocol details - 3GPP TS 29.229

Online References

1. [Diameter Base Protocol](#), IETF RFC 6733
2. [Diameter Network Access Server Application](#), IETF RFC 4005
3. [Diameter Credit-Control Application](#), IETF RFC 4006