

CSCF Rx Interface

Call Session Control Function

INTERWORK DESCRIPTION

Copyright

© Ericsson AB 2013–2017. 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	Introduction	1
2	Interface Overview	3
2.1	Interface Role	3
2.2	Services	3
2.3	Encapsulation and Addressing	3
3	Procedures	5
3.1	AA-Request Command	5
3.2	AA-Answer Command	6
3.3	Session-Termination-Request Command	6
3.4	Session-Termination-Answer Command	6
3.5	Abort-Session-Request Command	7
3.6	Abort-Session-Answer Command	7
3.7	Error Handling	7
3.8	Usage Examples	8
4	Information Model	11
5	Formal Syntax	13
5.1	Diameter Header	13
5.2	Attribute-Value Pairs	19
6	Security Considerations	39
6.1	IPsec Tunnel	39
7	Related Standards	41





1 Introduction

This document specifies the Diameter-based Rx protocol used by the P-CSCF between the P-CSCF and the Policy and Charging Rules Function (PCRF).



2 Interface Overview

The Rx reference point is between the P-CSCF and the PCRF, see Figure 1. The protocol used on Rx is the Diameter protocol.

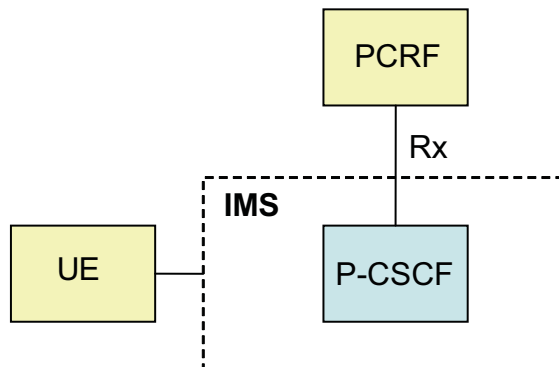


Figure 1 Interface Entities

2.1 Interface Role

This document describes the Rx reference point provided by the P-CSCF.

2.2 Services

The services offered by the CSCF are shown in Table 1.

Table 1 Offered Services

Offered Service	Description
Policy Control	The P-CSCF provides service for Policy Control

2.3 Encapsulation and Addressing

The P-CSCF Rx application protocol is used on top of the [RFC 3588 Diameter Base Protocol](#) specification.

The P-CSCF supports Diameter over IPv4 and SCTP or TCP.

2.3.1 Capability Exchange

At Diameter connection setup the P-CSCF and the PCRF advertise support for the 3GPP® vendor id (10415) by using Vendor-Id AVP in



Capability-Exchange-Request and Capability-Exchange-Answer commands.

2.3.2 Advertising Application Support

The standard 3GPP Rx application is defined as a vendor-specific Diameter application, where the vendor is the 3GPP, with the IANA-allocated Rx application identifier 16777236. The P-CSCF and the PCRF use this application identifier for Rx.

The P-CSCF and the PCRF advertise support for Rx by including the value of the standard Rx application (16777236) in the Auth-Application-Id AVP of the Capabilities-Exchange-Request and Capability-Exchange-Answer commands.

2.3.3 Re-Auth-Request

The P-CSCF supports reception of Re-Auth-Request (RAR), no special actions are taken and the RAR is responded with Result-Code 3001 (DIAMETER_COMMAND_NOT_SUPPORTED).



3 Procedures

Policy information is transferred between the P-CSCF and a PCRF using the AA-Request (AAR) and AA-Answer (AAA), Session-Termination-Request (STR) and Session-Termination-Answer (STA), and Abort-Session-Request (ASR) and Abort-Session-Answer (ASA) messages.

In the full Rx protocol, policy information is also transferred between the PCRF and the P-CSCF using the Re-Auth-Request (RAR) and Re-Auth-Answer (RAA) messages. These messages are not supported by the P-CSCF and are never processed.

Session-related policy data is sent whenever media is (re-)negotiated. The AAR message is used to transmit the policy information to the PCRF, which by replying with the AAA message confirms AAR reception.

An Rx session is started when the P-CSCF issues an initial AAR to the Rx Diameter server (PCRF), which by replying with the AAA message confirms AAR reception. The PCRF is to store the Session-Id, Origin-Host, and Origin-Realm from the received message to be able to send messages within the established session to the corresponding Diameter peer. The P-CSCF also stores the Orig-Host name received in an initial AAA answer from the PCRF.

An Rx session is modified when the P-CSCF issues a subsequent AAR to the PCRF using the same Session-Id as in the initial AAR message.

An Rx session is terminated when the Rx Diameter client (P-CSCF) issues an STR to the Rx Diameter server (PCRF), which by replying with the STA message confirms STR reception.

The PCRF can send the ASR message to the P-CSCF to inform it that the bearer for the established session is no longer available. The P-CSCF must acknowledge the command by sending an Abort-Session-Answer (ASA) command to the PCRF and terminate the policy session. The P-CSCF must indicate the termination of the policy session as stated in the previous paragraph.

3.1 AA-Request Command

The P-CSCF sends an AAR command when an Rx session is established or when an existing Rx session is to be modified with new or modified SDP information.

The important parameters sent by the P-CSCF in the AAR command are the following:

- Charging-Identifier
- Flow-Status
- Framed-IP-Address



- Max-Requested-Bandwidth-DL
- Max-Requested-Bandwidth-UL
- Media-Type
- Session-Id
- Subscription-ID

3.2 AA-Answer Command

The P-CSCF validates the received AA-Answer command (AAA) against the sent AAR messages by inspecting the following parameters:

- Result Code
- Session-Id

If the validation fails for one of these parameters or if the P-CSCF does not receive the AAA in time, the P-CSCF terminates the policy session. As a consequence, it terminates the SIP session, unless the P-CSCF is configured to allow SIP sessions to continue in case of Rx failure.

3.3 Session-Termination-Request Command

When the P-CSCF decides to terminate the Diameter session between P-CSCF and PCRF, the P-CSCF issues a Session-Termination-Request command indicating to PCRF that the Diameter session is terminated. The command includes an indication why the Diameter session is terminated.

The important parameters in the command are the following:

- Session-Id
- Termination-Cause

3.4 Session-Termination-Answer Command

The P-CSCF validates the received Session-Termination-Answer command (STA) against the sent STR messages by inspecting the following parameter:

- Session-Id

The P-CSCF ignores the STA if the validation fails, or no STA is received in time.



3.5 Abort-Session-Request Command

The P-CSCF validates the received `Abort-Session-Request` command (ASR) by inspecting the following parameters:

- `Abort Cause`
- `Session-Id`

If the validation fails for one of these parameters, the SIP session within the P-CSCF does not terminate.

3.6 Abort-Session-Answer Command

At reception of ASR command, the P-CSCF returns an `Abort-Session-Answer` (ASA) command indicating the result of the ASR message processing. The following parameters are the most important:

- `Result-Code`
- `Session-Id`

3.7 Error Handling

The Diameter connection is supervised and when no activity is detected watchdog requests are sent. When no watchdog answer or any other message is received on that connection, it is considered down, closed.

Attempts are always made to reopen closed connections. Three watchdog requests are sent after a successful re-connection and the Diameter connection is considered up after three successful watchdog requests.

If a request from the P-CSCF is not answered within a configurable time, the request is retransmitted a configurable number of times. If there are multiple peers specified for the destination realm, the message is sent to an alternative and available peer that serves the application on the realm.

The time for which the P-CSCF waits for an Rx answer message is controlled through parameters in the P-CSCF and the Diameter stack. If the Diameter stack is not able to establish a connection to the PCRF, or if it does not receive an Rx answer message in time, it sends an error notification to the P-CSCF application. If the delayed response message arrives after the time-out, the Diameter stack discards the message.

When the P-CSCF sends an AAR to the PCRF over the Rx interface, the P-CSCF terminates the SIP session if one of the following happens, unless the SIP Session Continue feature is enabled:

- The P-CSCF receives an AAA with a negative result code in a `Result-Code AVP`.



- The P-CSCF receives an AAA message that contains an Experimental-Result-Code AVP.
- The P-CSCF receives an AAA message that does not contain the Result-Code or Experimental-Result-Code AVP. As a result, it receives an error notification from the Diameter stack.
- The P-CSCF does not receive an AAA message.

If the SIP Session Continue feature is enabled, and the Rx session could not be established successfully, the P-CSCF allows the SIP session to continue without maintaining an associated Rx session. If an Rx session could not be created successfully at the establishment of the SIP session, the P-CSCF assumes that the media session is “best effort”. Hence, if possible, the P-CSCF terminates the Rx session, and it does not invoke the PCRF for that SIP session again. If an Rx session has been created successfully at the establishment of the SIP session or the receipt of an initial SDP answer, the P-CSCF continues to send update AARs for SIP session modifications and an STR at SIP session termination, even if any of the update AARs fails.

If a Diameter request message is received with an AVP that is not known to the P-CSCF and the unknown AVP has the “M” bit set in the AVP header, the P-CSCF rejects the message with the result code `DIAMETER_AVP_UNSUPPORTED`.

If the P-CSCF receives an answer with an unknown Result-Code, the P-CSCF treats the message as described in Section 5.2.1.7 Result-Code on page 22.

If the P-CSCF receives a message not included in Section 4 on page 11, the message is ignored.

3.8 Usage Examples

Note: The examples are not complete especially from a SIP and Rx message interaction point of view and that node like the HSS is excluded as they are not relevant in this context.

3.8.1 Session Establishment

The sequence in Figure 2 is an example of a SIP session setup and the interaction with the Rx interface.

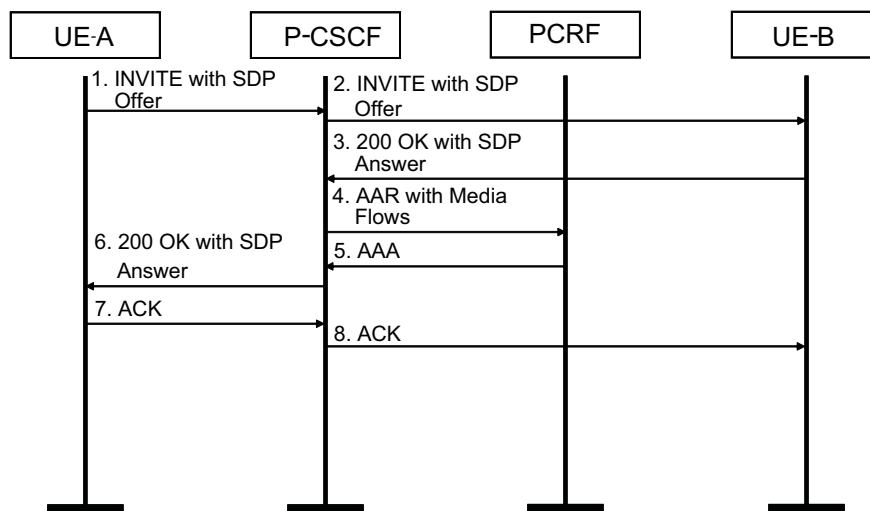


Figure 2 Session Establishment

3.8.2

Session Disconnection

The sequence in Figure 3 is an example of a release of a SIP session and the interaction with the Rx interface.

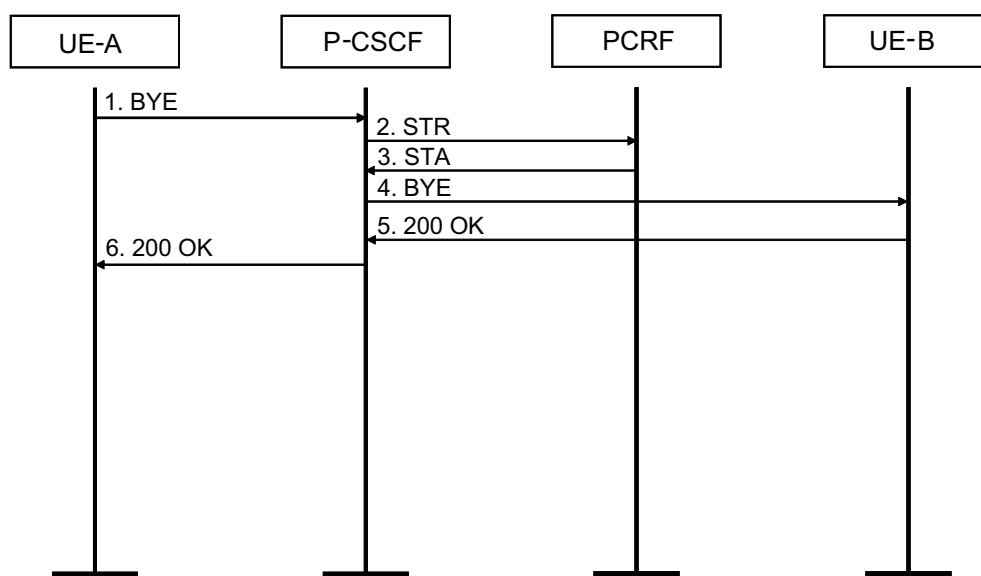


Figure 3 Session Disconnection

3.8.3

Abort Session

The sequence in Figure 4 is an example of when the PCRF ends a session that results in that the P-CSCF terminates the SIP session and Rx session.

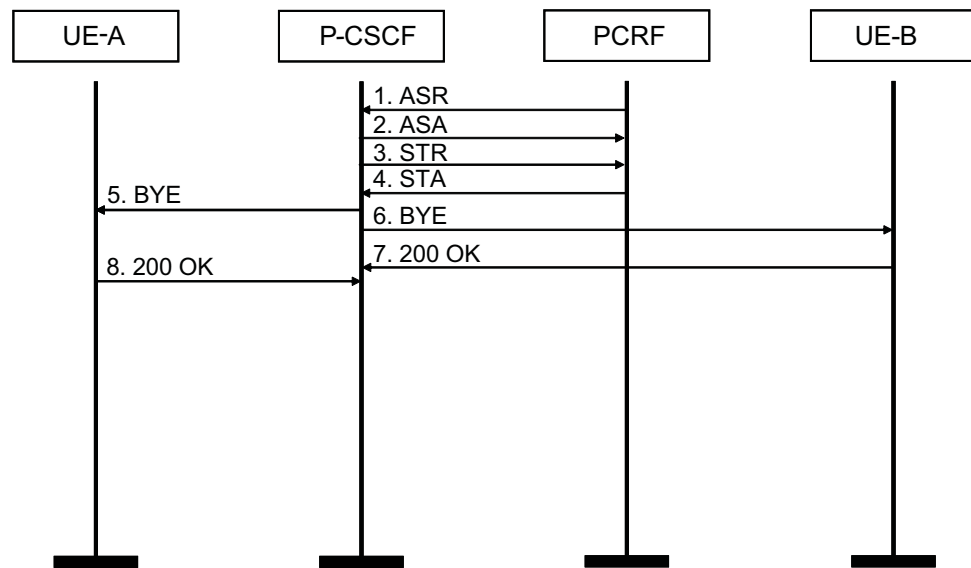


Figure 4 Abort Session



4 Information Model

The six Diameter policy messages that are used in the P-CSCF have the command codes defined in Table 2.

Table 2 Commands Used on Rx Interface

Command Name	Code	Code Direction
AA-Request	265	P-CSCF to PCRF
AA-Answer	265	PCRF to P-CSCF
Session-Termination-Request	275	P-CSCF to PCRF
Session-Termination-Answer	275	PCRF to P-CSCF
Abort-Session-Request	274	PCRF to P-CSCF
Abort-Session-Answer	274	P-CSCF to PCRF



5 Formal Syntax

The following symbols are used in this document:

- **< AVP >** indicates a mandatory AVP with a fixed position in the message.
- **{ AVP }** indicates a mandatory AVP in the message.
- **[AVP]** indicates an optional AVP in the message.
- *** AVP** indicates that multiple occurrences of an AVP are possible.

5.1 Diameter Header

A Diameter header has the format as shown in Figure 5.

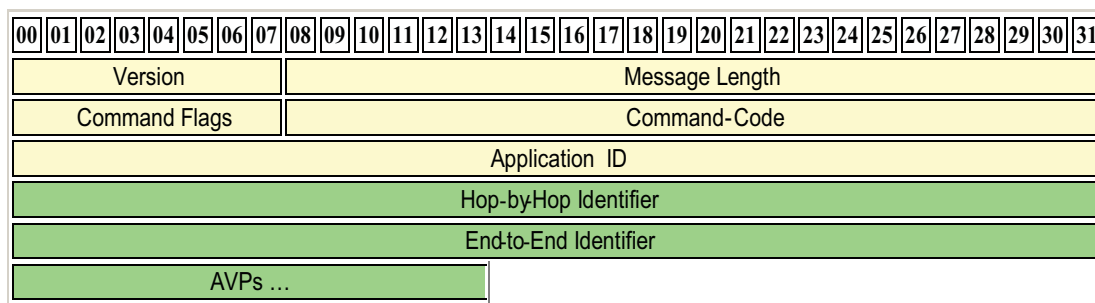


Figure 5 Diameter Header

- Version, 8 bits**

The Diameter version, set to 1.
- Message, 24 bits**

The length of the Diameter message including the header field.

Command Flags, 8 bits

See Figure 6.

- **R** – Set to 1 if the message is an AAR or STR message as described in Table 2.

Set to 0 if the message is an ASA message as described in Table 2.

Expected to have the value 0 if the message is an AAA or an STA message as described in Table 2.

Expected to have the value 1 if the message is an ASR message as described in Table 2.

- **P** – Set to 1 if the message is proxiable.

Always set to 1 in all messages described in Section 5.1.1 AA-Request Command on page 15 to Section 5.1.6 Abort-Session-Answer Command on page 18.

- **E** – Expected to have the value 1 if the message is an AAA, STA, or ASA and contains Protocol Error 3xxx as described in the [RFC 3588 Diameter Base Protocol](#) specification.

Expected to have the value 0 if the message is an AAA, STA, or ASA and do not contain Protocol Error 3xxx.

- **T** – Set to 1 if re-Transmitted message.

Always set to 0.

- **Reserved** – Not used (set to 0).

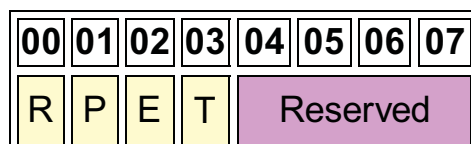


Figure 6 Diameter Command Flags

Command-Code, 24 bits

The command used in Diameter Policy messages.

Application-ID, 32 bits

A specific Diameter Application, always set to 3GPP Rx 16777236.



Hop-by-Hop Identifier, 32 bits

An unsigned integer generated by the P-CSCF. This integer is unique on a given connection at any given time with same value found in the answer message and the corresponding request.

End-to-End Identifier, 32 bits

An unsigned integer used to detect duplicate messages. This integer is generated by the P-CSCF and remains locally unique for at least 4 minutes with same value found in the answer message and the corresponding request.

5.1.1 AA-Request Command

The Diameter AA-Request (AAR) command is used for sending the P-CSCF policy information to the PCRF server. The format of the AA-Request command is listed in Table 3.

Table 3 AA-Request Content

AVP	AVP Code	Value Type
Diameter Base Protocol AVPs⁽¹⁾		
< Session-Id >	263	UTF8String
{ Auth-Application-Id }	258	Unsigned32
{ Origin-Host }	264	DiameterIdentity
{ Origin-Realm }	296	DiameterIdentity
{ Destination-Realm }	283	DiameterIdentity
[Destination-Host]	293	DiameterIdentity
[Framed-IP-Address]	8	OctetString
[Subscription-id]	443	Grouped
→ { Subscription-Id-Type }	450	Enumerated
→ { Subscription-Id-Data }	444	UTF8String
* [AVP]		
3GPP Diameter Rx AVPs⁽²⁾		
[AF-Charging-Identifier]	505	OctetString
1 * [Media-Component-Description]	517	Grouped
→ { Media-Component-Number }	518	Unsigned32
→ * [Media-Sub-Component]	519	Grouped
→→ { Flow-Number }	509	Unsigned32
→→ 0 * 2 [Flow-Description]	507	IPFilterRule

Table 3 AA-Request Content

AVP	AVP Code	Value Type
→→ [Flow-Usage]	512	Enumerated
→ [Media-Type]	520	Enumerated
→ [Max-Requested-Bandwidth-DL]	515	Unsigned32
→ [Max-Requested-Bandwidth-UL]	516	Unsigned32
→ [Flow-Status]	511	Enumerated
→ [RR-Bandwidth]	521	Unsigned32
→ [RS-Bandwidth]	522	Unsigned32
→ [AF-Application-Identifier]	504	OctetString
→ * [Codec-Data]	524	OctetString
[SIP-Forking-Indication]	523	Enumerated

(1) These AVPs are extracted from [RFC 3588](#) or [RFC 4006](#).

(2) Extracted from [3GPP TS 29.214](#).

5.1.2 AA-Answer Command

The AA-Answer command is sent by the PCRF to the P-CSCF as a response to the AAR message specified in Section 5.1.1 AA-Request Command on page 15.

The AVPs that are supported in an AA-Answer are listed in Table 4.

Table 4 AA-Answer Content

AVP	Code	Type
Diameter Base Protocol AVPs⁽¹⁾		
< Session-Id >	263	UTF8String
{ Auth-Application-Id }	258	Unsigned32
{ Origin-Host }	264	DiameterIdentity
{ Origin-Realm }	296	DiameterIdentity
{ Result-Code }	268	Unsigned32
* [AVP]		
3GPP Diameter Rx AVPs⁽²⁾		
[Experimental-Result]	297	Grouped
→ { Experimental-Result-Code }	298	Unsigned32

(1) Extracted from [RFC 3588](#).

(2) Extracted from [3GPP TS 29.214](#).



5.1.3 Session-Termination-Request Command

The Session-Termination-Request (STR) command is used to terminate an Rx session between the P-CSCF and the PCRF. The format of the Session-Termination-Request command is listed in Table 5.

Table 5 Session-Termination-Request Content

AVP	Code	Type
Diameter Base Protocol AVPs⁽¹⁾		
< Session-Id >	263	UTF8String
{ Origin-Host }	264	DiameterIdentity
{ Origin-Realm }	296	DiameterIdentity
{ Destination-Realm }	283	DiameterIdentity
{ Termination-Cause }	295	Enumerated
{ Auth-Application-Id }	258	Unsigned32
[Destination-Host]	293	DiameterIdentity
* [AVP]		

(1) Extracted from [RFC 3588](#).

5.1.4 Session-Termination-Answer Command

The Session-Termination-Answer command (STA) is sent by the PCRF to the P-CSCF to respond to the STR specified in Section 5.1.3 Session-Termination-Request Command on page 17. The AVPs that are supported in a Session-Termination-Answer are listed in Table 6.

Table 6 Session-Termination-Answer Content

AVP	Code	Type
Diameter Base Protocol AVPs⁽¹⁾		
< Session-Id >	263	UTF8String
{ Origin-Host }	264	DiameterIdentity
{ Origin-Realm }	296	DiameterIdentity
{ Result-Code }	268	Unsigned32
* [AVP]		

(1) Extracted from [RFC 3588](#).



5.1.5 Abort-Session-Request Command

The Abort-Session-Request (ASR) command is sent by the PCRF to inform the P-CSCF that the bearer for the established session is no longer available. The format of the Abort-Session-Request message is listed in Table 7.

Table 7 Abort-Session-Request Content

AVP	Code	Type
Diameter Base Protocol AVPs⁽¹⁾		
< Session-Id >	263	UTF8String
{ Origin-Host }	264	DiameterIdentity
{ Origin-Realm }	296	DiameterIdentity
{ Destination-Realm }	283	DiameterIdentity
[Destination-Host]	293	DiameterIdentity
{ Auth-Application-Id }	258	Unsigned32
* [AVP]		
3GPP Diameter Rx AVPs⁽²⁾		
{ Abort-Cause }	500	Enumerated

(1) Extracted from [RFC 3588](#).

(2) Extracted from [3GPP TS 29.214](#).

5.1.6 Abort-Session-Answer Command

The Abort-Session-Answer (ASA) command is sent by the P-CSCF to respond to the ASR specified in Section 5.1.5 Abort-Session-Request Command on page 18. The AVPs that are supported in an Abort-Session-Answer are listed in Table 8.

Table 8 Abort-Session-Answer Content

AVP	Code	Type
Diameter Base Protocol AVPs⁽¹⁾		
< Session-Id >	263	UTF8String
{ Origin-Host }	264	DiameterIdentity
{ Origin-Realm }	296	DiameterIdentity
{ Result-Code }	268	Unsigned32
* [AVP]		

(1) Extracted from [RFC 3588](#).

5.2 Attribute-Value Pairs

A Diameter AVP header has the format shown in Figure 7.

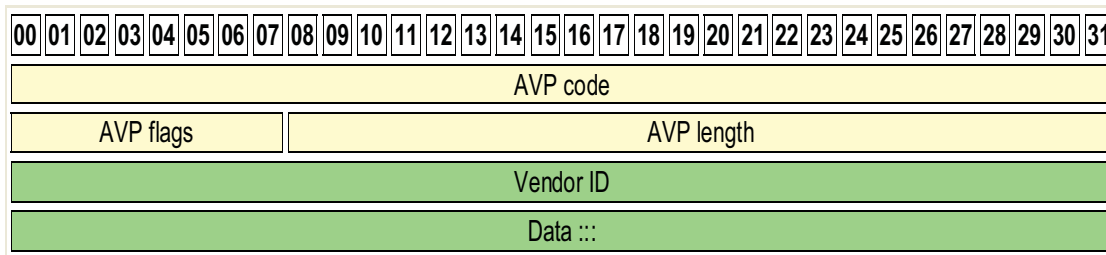


Figure 7 Diameter AVP Header

AVP Code Indicates, together with the optional information element Vendor ID, the current AVP. Supported AVP elements are listed in Section 5.2.1 Diameter Base Protocol AVPs on page 20 and Section 5.2.2 3GPP Diameter Policy AVPs on page 27.

AVP Flags For details, refer to [RFC 3588 Diameter Base Protocol](#). See also Section 5.2.1 Diameter Base Protocol AVPs on page 20, and Section 5.2.2 3GPP Diameter Policy AVPs on page 27.

R	Reserved
P	Indicates the need for encryption for end-to-end security
M	Indicates whether support of the AVP is required. If an AVP with the “M” bit set is received by a Diameter client, server, proxy, or translation agent and either the AVP or its value is unrecognized, the message MUST be rejected. Diameter Relay and redirect agents MUST NOT reject.
V	The Vendor-Specific bit, indicates whether the optional Vendor-ID field is present in the AVP header. When set, the AVP Code belongs to the specific vendor code address space.

AVP Length The length of the AVP (number of octets) including the header. For details, refer to [RFC 3588 Diameter Base Protocol](#).



Vendor ID Optional in the AVP header, if present it specifies the vendor that defined the AVP. For details, refer to [RFC 3588 Diameter Base Protocol](#).

In the following sections, the AVPs are split up into the following groups:

- Diameter Base Protocol AVPs, derived from [RFC 3588 Diameter Base Protocol](#)
- 3GPP Diameter Policy AVPs, derived from [3GPP TS 29.214 7.0.0 Policy and Charging Control over Rx reference point](#)

5.2.1 Diameter Base Protocol AVPs

This section describes the Diameter Base Protocol AVPs, which are derived from the [RFC 3588 Diameter Base Protocol](#) and [RFC 4005 Diameter Network Access Server Application](#) standards.

5.2.1.1 Auth-Application-Id

The Auth-Application-Id AVP, see Table 9, is used to advertise support of the Authentication and Authorization portion of an application. It occurs in every AAR and STR and is expected in every AAA and ASR. The value is set to 16777236, which is the application ID used by the Rx interface.

Table 9 Auth-Application-Id

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	258	12	Unsigned32

5.2.1.2 Destination-Host

Messages including the Destination-Host AVP, see Table 10, are addressing a specific Diameter Peer. The value Destination-Host AVP is either obtained from the Origin-Host AVP from a previous message, within the same Policy Session, or Destination-Host AVP can also be present in an initial message, if a specific peer is addressed. The absence of the Destination-Host AVP causes a message to be sent to any Diameter server supporting the application within the realm specified in Destination-Realm AVP.

Table 10 Destination-Host AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	293	> 8	DiameterIdentity

Example

```
neighbour1.ericsson.se
```




5.2.1.3 Destination-Realm

The Destination-Realm AVP, see Table 11, contains the realm the message is to be routed to. The Destination-Realm must be present in all Diameter Policy Request messages.

Table 11 Destination-Realm AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	283	> 8	DiameterIdentity

The value is extracted from local configuration.

Example

```
pcrf.telia.com
```

5.2.1.4 Framed-IP-Address

The Framed-IP-Address AVP, see Table 12, contains the valid routable IPv4 address that is applicable for the IP Flows to the UE. The PCRF uses this address to identify the correct IP-CAN session (session binding). The values 0xFFFFFFFF (255.255.255.255) and 0xFFFFFFF0 (255.255.255.254) are not applicable as described in the [RFC 4005 Diameter Network Access Server Application](#) and [RFC 2865 Remote Authentication Dial In User Service \(RADIUS\)](#) specifications.

The IP address is formatted as four octets, the most significant octet first.

Table 12 Framed-IP-Address AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	8	12	OctetString

Example

```
C0 A8 01 10 (192.168.1.16)
```

5.2.1.5 Origin-Host

The Origin-Host AVP, see Table 13, identifies where the Diameter message originated. The value of the Origin-Host AVP must uniquely identify a single host.

Table 13 Origin-Host AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	264	> 8	DiameterIdentity



Example

```
pcscf.ericsson.se
```

5.2.1.6

Origin-Realm

The Origin-Realm AVP, see Table 14, contains the Realm of the originator of any Diameter message and must be present in all messages. The P-CSCF Origin-Realm is set by configuration.

Table 14 Origin-Realm AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	296	> 8	DiameterIdentity

Example

```
ericsson.se
```

5.2.1.7

Result-Code

The Result-Code AVP, see Table 15, indicates whether a particular request was completed successfully or whether an error occurred.

Table 15 Result-Code AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	268	12	Unsigned32

All Diameter AA-Answer messages (AAAs), Abort-Session-Answer messages (ASAs), and Session-Termination-Answer (STAs) must include one Result-Code AVP. The classes of errors provided by [RFC 3588 Diameter Base Protocol](#) and the actions taken by P-CSCF for each error class are described in Table 16. Any P-CSCF action “Policy Session Termination” terminates the ongoing SIP service, unless the SIP Session Continue function is enabled.

Table 16 Diameter Error Classes

Result Class	Description	CSCF Action
1XXX	Informational	Policy Session Termination
2XXX	DIAMETER_SUCCESS	Process the AAA or STA message
3XXX	DIAMETER_ERROR	Policy Session Termination
4XXX	TRANSIENT_FAILURE	Policy Session Termination
5XXX	PERMANENT_FAILURE	Policy Session Termination
OTHER	Unknown Result Code	Policy Session Termination



For detailed examples for each class of error, refer to Section 7.1 in the [RFC 3588 Diameter Base Protocol](#) specification.

Messages with Result Class Informational are treated as unexpected Result-Code and results in that the Policy Session is terminated.

Valid Result-Codes:

— DIAMETER_SUCCESS (2001)

The request was successfully completed.

— DIAMETER_COMMAND_UNSUPPORTED (3001)

The request contained a Command-Code that the receiver did not recognize or support. This must be used when a Diameter node receives an experimental command that it does not understand.

— DIAMETER_UNABLE_TO_DELIVER (3002)

This result code is returned if the Diameter stack cannot deliver the message to the destination, either because no host within the realm supporting the required application was available to process the request, or because Destination-Host AVP was given without the associated Destination-Realm AVP.

— DIAMETER_REALM_NOT_SERVED (3003)

The intended realm of the request is not recognized.

— DIAMETER_APPLICATION_UNSUPPORTED (3007)

A request was sent for an application that is not supported.

— DIAMETER_INVALID_HDR_BITS (3008)

A request was received whose bits in the Diameter header were either set to an invalid combination, or to a value that is inconsistent with the definition of the command code.

— DIAMETER_INVALID_AVP_BITS (3009)

A request was received that included an AVP whose flag bits are set to an unrecognized value, or that is inconsistent with the definition of the AVP.

— DIAMETER_UNKNOWN_PEER (3010)

A CER was received from an unknown peer.

— DIAMETER_AVP_UNSUPPORTED (5001)

The peer received a message that contained an AVP that is not recognized or supported and was marked with the Mandatory bit. A Diameter message



with this error must contain one or more Failed-AVP AVP containing the AVPs that caused the failure.

— DIAMETER_UNKNOWN_SESSION_ID (5002)

The request contained an unknown Session-Id.

— DIAMETER_AUTHORIZATION_REJECTED (5003)

A request was received for which the user could not be authorized. This error could occur if the service requested is not permitted to the user.

— DIAMETER_INVALID_AVP_VALUE (5004)

The request contained an AVP with an invalid value in its data portion. A Diameter message indicating this error must include the offending AVPs within a Failed-AVP AVP.

— DIAMETER_INVALID_AVP_VALUE (5004)

The request contained an AVP with an invalid value in its data portion. A Diameter message indicating this error must include the offending AVPs within a Failed-AVP AVP.

— DIAMETER_MISSING_AVP (5005)

The request did not contain an AVP that is required by the Command Code definition. If this value is sent in the Result-Code AVP, a Failed-AVP AVP can be included in the message. The Failed-AVP AVP must contain an example of the missing AVP complete with the Vendor-Id if applicable. The value field of the missing AVP can be of correct minimum length and contain zeroes.

— DIAMETER_RESOURCES_EXCEEDED (5006)

A request was received that cannot be authorized because the user has already expended allowed resources. An example of this error condition is a user that is restricted to one dial-up PPP port, attempts to establish a second PPP connection.

— DIAMETER_AVP_NOT_ALLOWED (5008)

A message was received with an AVP that must not be present. The Failed-AVP AVP must be included and contain a copy of the offending AVP.

— DIAMETER_AVP_OCCURS_TOO_MANY_TIMES (5009)

A message was received that included an AVP that appeared more often than permitted in the message definition. The Failed-AVP AVP must be included and contain a copy of the first instance of the offending AVP that exceeded the maximum number of occurrences.

— DIAMETER_NO_COMMON_APPLICATION (5010)

This error is returned when a CER message is received, and there are no common applications supported between the peers.

— **DIAMETER_UNSUPPORTED_VERSION** (5011)

This error is returned when a request was received, whose version number is unsupported.

— **DIAMETER_UNABLE_TO_COMPLY** (5012)

This error is returned when a request is rejected for unspecified reasons.

— **DIAMETER_INVALID_BIT_IN_HEADER** (5013)

This error is returned when an unrecognized bit in the Diameter header is set to one (1).

— **DIAMETER_INVALID_AVP_LENGTH** (5014)

The request contained an AVP with an invalid length. A Diameter message indicating this error must include the offending AVPs within a **Failed-AVP** AVP.

— **DIAMETER_INVALID_MESSAGE_LENGTH** (5015)

This error is returned when a request is received with an invalid message length.

— **DIAMETER_NO_COMMON_SECURITY** (5017)

This error is returned when a CER message is received, and there are no common security mechanisms supported between the peers. A **Capabilities-Exchange-Answer** (CEA) must be returned with the **Result-Code** AVP set to **DIAMETER_NO_COMMON_SECURITY**.

5.2.1.8

Session-Id

The **Session-Id** AVP, see Table 17, is used to identify a specific session. All messages pertaining to a specific session must include only one **Session-Id** AVP and the same value must be used throughout the life of a policy session. The **Session-Id** is created by the P-CSCF initiating the policy session.

Table 17 Session-Id AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	263	>8	UTF8String

Grammar:

```
< Cscf Rx Orig Host >; < Public Id >;
  < Hashed callId >; < Hashed toTag >
```



Example

```
pcscf.abcdef.com;subscriber@example.com;89071234;12235234
```

5.2.1.9 Termination-Cause

The Termination-Cause AVP, see Table 18, is of type Enumerated and it is used to indicate the reason why a session was terminated. The Termination-Cause must be present in STR messages.

Table 18 Termination-Cause AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	295	12	Enumerated

Defined values:

— DIAMETER_LOGOUT (1)

The user initiated a disconnect.

— Not used 2–8

The P-CSCF always sends the value DIAMETER_LOGOUT (1) in the Session-Termination-Request (STR).

5.2.1.10 Subscription-Id

The Subscription-Id AVP, see Table 19, is used to identify the subscription of the end user and is of type Grouped.

Table 19 Subscription-Id AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	433	>8	Grouped

The Subscription-Id AVP includes a Subscription-Id-Data AVP that holds the identifier and a Subscription-Id-Type AVP that defines the identifier type.

Grammar:

```
< Subscription-Id > ::= < AVP Header: 443 >  
    { Subscription-Id-Type }  
    { Subscription-Id-Data }
```

5.2.1.11 Subscription-Id-Type

The Subscription-Id-Type AVP, see Table 20, is used to determine which type of identifier is carried by the Subscription-Id-Data AVP.



Table 20 Subscription-Id-Type AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	450	12	Enumerated

Defined values:

— END_USER_E164 (0)

The identifier is in international E.164 format, for example, MSISDN, according to the ITU-T E.164 numbering plan defined in [E164] and [CE164].

— Not used 1

— END_USER_SIP_URI (2)

The identifier is in the form of a SIP URI, as defined in [RFC 3261 Session Initiation Protocol](#).

— Not used 3–4

5.2.1.12

Subscription-Id-Data

The Subscription-Id-Data AVP, see Table 21, is used to identify the end user and is of type UTF8String. This AVP contains the IMS Public User Identity of the end user.

Table 21 Subscription-Id-Data AVP

V	M	P	AVP Code	AVP Length	AVP Data Type
0	1	0	444	> 8	UTF8String

Example

```
- Case of END_USER_SIP_URI:
sip:champions@degerforsif.se
- Case of END_USER_E164:
4687190037
```

5.2.2

3GPP Diameter Policy AVPs

This section describes the 3GPP Diameter Policy AVPs, which are derived from the [3GPP TS 29.214 7.0.0 Policy and Charging Control over Rx reference point](#) specification.



5.2.2.1 AF-Charging-Identifier

The AF-Charging-Identifier AVP, see Table 22, contains the IMS Charging Identifier that is being used by the P-CSCF. This information can be used for charging correlation with the bearer layer.

Table 22 AF-Charging-Identifier AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	505	>8	OctetString	10415

5.2.2.2 Media-Component-Description

The Media-Component-Description AVP, see Table 23, is a grouped AVP. It contains service information for a single media component (media flow) within a SIP session. It can be based on the Session Description Information (SDI) exchanged between the end-points through the P-CSCF. The information can be used by the server to determine authorized QoS and IP flow classifiers for bearer authorization and charging rule selection.

Table 23 Media-Component-Description AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	517	>12	Grouped	10415

Within one Diameter message, a single IP flow must not be described by more than one Media-Component-Description AVP.

Bandwidth information and Flow-Status information provided within the Media-Component-Description AVP applies to all those IP flows within the media component for which no corresponding information is being provided within Media-Sub-Component AVPs.

If a Media-Component-Description AVP is not supplied, or if optional AVPs within a Media-Component-Description AVP are omitted, but corresponding information has been provided in previous Diameter messages, the previous information for the corresponding IP flows remains valid.

All IP flows within a Media-Component-Description AVP are permanently disabled by supplying a Flow Status AVP with value REMOVED.

Each Media-Component-Description AVP must contain either zero, or two Codec-Data AVPs. If the SDP offer-answer procedures of [RFC 3264 An Offer/Answer Model with the Session Description Protocol \(SDP\)](#) are applicable for the session negotiation between the two ends taking part in the communication (for example, for IMS), the following applies:

- The P-CSCF provides information that is derived from an SDP answer and from the corresponding SDP offer.



- If the Media-Component-Description AVP contains two Codec-Data AVPs, one of them represents an SDP offer and the other one the corresponding SDP answer.

Note: Some SDP parameters for the same codec in the SDP offer and answer are independent of each other and refer to IP flows in opposite directions, for instance, some MIME parameters conveyed within “a=fmtp” SDP lines and the packetization time within the “a=ptime” line. Other parameters within the SDP answer take precedence over corresponding parameters within the SDP offer.

Grammar:

```
Media-Component-Description ::= < AVP Header: 517 >
    { Media-Component-Number }
    * [ Media-Sub-Component ]
    [ Media-Type ]
    [ Max-Requested-Bandwidth-DL ]
    [ Max-Requested-Bandwidth-UL ]
    [ Flow-Status ]
    [ RR-Bandwidth ]
    [ RS-Bandwidth ]
    [ AF-Application-Identifier ]
    * [ Codec-Data ]
```

5.2.2.3

Media-Component-Number

The Media-Component-Number AVP, see Table 24, contains the ordinal number of the media component, assigned according to the rules in Annex C of the [3GPP TS 29.207 6.5.0 Policy control over Go interface](#) specification.

Table 24 Media-Component-Number AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	518	12	Unsigned32	10415

5.2.2.4

Media-Sub-Component

The Media-Sub-Component AVP, see Table 25, is a Grouped AVP. It contains the requested QoS and filters for the set of IP flows identified by their common Flow-Identifier. The Flow-Identifier is defined in the [3GPP TS 29.207 6.5.0 Policy control over Go interface](#) specification.

Table 25 Media-Sub-Component AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	519	>12	Grouped	10415



If a Media-Sub-Component AVP is not supplied, or if optional AVPs within a Media-Sub-Component AVP are omitted, but corresponding information has been provided in previous Diameter messages, the previous information for the corresponding IP flows remains valid, unless new information is provided within the encapsulating Media-Component-Description AVP. If Flow-Description AVPs are supplied, they replace all previous Flow-Description AVPs, even if a new Flow-Description AVP has the opposite direction as the previous Flow-Description AVP.

All IP flows within a Media-Sub-Component AVP are permanently disabled by supplying a Flow Status AVP with value REMOVED. The server can delete corresponding filters and state information.

Grammar:

```
Media-Sub-Component ::= < AVP Header: 519 >
                        { Flow-Number }
                        0*2[ Flow-Description ]
                        [ Flow-Usage ]
```

5.2.2.5 Flow-Number

The Flow-Number AVP, see Table 26, contains the ordinal number of the IP flows, assigned according to the rules in annex C of the [3GPP TS 29.207 6.5.0 Policy control over Gx interface](#) specification.

Table 26 Flow-Number AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	509	12	Unsigned32	10415

5.2.2.6 Flow-Description

The Flow-Description AVP, see Table 27, is of type IPFilterRule. It defines a packet filter for an IP flow with the following information:

- Direction (in or out)
- Source and destination IP address (possibly masked)
- Protocol
- Source and destination port

The Source Port can be omitted to indicate that any source port is allowed. For the Rx interface, lists or ranges are not to be used.



Table 27 Flow-Description AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	507	> 20	IPFilterRule	10415

The IPFilterRule type must be used with the following restrictions:

- Only the Action “permit” is to be used.
- No “options” are to be used.
- The invert modifier “!” for addresses is not to be used.
- The keyword “assigned” is not to be used.

For the Rx interface, the Flow-Description AVP must be used to describe a single IP flow.

The direction “in” refers to uplink IP flows, and the direction “out” refers to downlink IP flows.

The IP-Filter-Rule is of type OctetString and is formatted as shown in the following example:

```
; Start of ABNF description of Rx IP-Filter-Rule
ip-filter-rule = "permit" " "
                ("in" / "out" / "inout") " "
                ("ip" / ip-proto) filter-body
ip-proto       = d8 ; tcp (6), udp (17)
filter-body    = " from " ip-address [" " layer4-port]
                " to " ip-address [" " layer4-port]
ip-address     = (ipv4-address ["/" ipv4mask] /
                "any")
ipv4-address   = d8 "." d8 "." d8 "." d8
ipv4mask       = DIGIT ; 0-9
                / %x31-32 DIGIT ; 10-29
                / "3" %x30-32 ; 30-32
DIGIT          = %x30-39 ; 0-9
layer4-port    = d16
d8             = DIGIT ; 0-9
                / %x31-39 DIGIT ; 10-99
                / "1" 2DIGIT ; 100-199
                / "2" %x30-34 DIGIT ; 200-249
                / "25" %x30-35 ; 250-255
d16            = DIGIT ; 0-9
                / %x31-35 1*4DIGIT ; 10-59999
                / "6" "4" 3DIGIT ; 60000-64999
                / "6" "5" %x30-34 2DIGIT ; 65000-65499
                / "6" "5" "5" %x30-32 DIGIT ; 65500-65529
                / "6" "5" "5" "3" %x30-36 ; 65530-65536
```

Example 1 Permit Input IP from 10.11.12.13 to 13.12.11.10



5.2.2.7 Flow-Usage

The Flow-Usage AVP, see Table 28, provides information about the use of IP Flows.

Table 28 Flow-Usage AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	512	12	Enumerated	10415

Defined values:

— NO_INFORMATION (0)

No information about the use of the IP flow is being provided.

— RTCP (1)

An IP flow is used to transport RTCP.

— NO_INFORMATION

Default value.

Note: An AF can choose not to identify RTCP flows, for example, to avoid that RTCP flows are always enabled by the server.

5.2.2.8 Media-Type

The Media-Type AVP, see Table 29, determines the media type of a session component. The Media-Type indicate the type of media in the same way as the SDP media types with the same names defined in the [RFC 2327 SDP: Session Description Protocol](#) specification.

Table 29 Media-Type AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	520	12	Enumerated	10415

Defined types:

— AUDIO (0)

— VIDEO (1)

— DATA (2)

— APPLICATION (3)

— CONTROL (4)

— TEXT (5)



— MESSAGE (6)

— OTHER (0xFFFFFFFF)

Note: Ericsson also supports the following three types for media types that are not defined by 3GPP:

- MODEL (0xF0000001)
- MULTIPART (0xF0000002)
- IMAGE (0xF0000003)

5.2.2.9 Max-Requested-Bandwidth-DL

The Max-Requested-Bandwidth-DL AVP, see Table 30, indicates the maximum requested bandwidth in bits per second for a downlink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, for example IP, UDP, RTP, and RTP payload.

Table 30 Max-Requested-Bandwidth-DL AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	515	12	Unsigned32	10415

5.2.2.10 Max-Requested-Bandwidth-UL

The Max-Requested-Bandwidth-UL AVP, see Table 31, indicates the maximum requested bandwidth in bits per second for an uplink IP flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, for example, IP, UDP, RTP, and RTP payload.

Table 31 Max-Requested-Bandwidth-UL AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	516	12	Unsigned32	10415

5.2.2.11 Flow-Status

The Flow-Status AVP, see Table 32, describes whether the IP flows are to be enabled or disabled.

Table 32 Flow-Status AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	511	12	Enumerated	10415



Defined values:

— ENABLED-UPLINK (0)

Enables associated uplink IP flows and to disable associated downlink IP flows

— ENABLED-DOWNLINK (1)

Enables associated downlink IP flows and to disable associated uplink IP flows

— ENABLED (2)

Enables all associated IP flows in both directions

— DISABLED (3)

Disables all associated IP flows in both directions

— REMOVED (4)

Remove all associated IP flows

5.2.2.12

RR-Bandwidth

The RR-Bandwidth AVP, see Table 33, indicates the maximum required bandwidth in bits per second for RTCP receiver reports within the session component, as specified in the [RFC 3566 Session Description Protocol \(SDP\) Bandwidth Modifiers for RTP Control Protocol \(RTCP\) Bandwidth](#) specification.

The bandwidth contains all the overhead coming from the IP-layer and the layers above, that is, IP, UDP, and RTCP.

Table 33 RR-Bandwidth AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	521	12	Unsigned32	10415

5.2.2.13

RS-Bandwidth

The RS-Bandwidth AVP, see Table 34, indicates the maximum required bandwidth in bits per second for RTCP sender reports within the session component, as specified in the [RFC 3566 Session Description Protocol \(SDP\) Bandwidth Modifiers for RTP Control Protocol \(RTCP\) Bandwidth](#) specification.

The bandwidth contains all the overhead coming from the IP-layer and the layers above, that is, IP, UDP, and RTCP.



Table 34 RS-Bandwidth AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	522	12	Unsigned32	10415

5.2.2.14

SIP-Forking-Indicator

The SIP-Forking-Indicator AVP, see Table 35, describes if several SIP dialogues are related to one Diameter session.

Table 35 SIP-Forking-Indicator AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	523	12	Enumerated	10415

Defined values:

— SINGLE_DIALOGUE (0)

The Diameter session relates to a single SIP dialogue. This is the default value applicable if the AVP is omitted.

— SEVERAL_DIALOGUES (1)

The Diameter session relates to several SIP dialogues.

5.2.2.15

Abort-Cause

The Abort-Cause AVP, see Table 36, is sent by the PCRF to inform the P-CSCF that bearer for the established UE session is no longer available. The value indicates the cause of an Abort-Session-Request (ASR) indicating a PDP context release.

Table 36 Abort-Cause AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	500	12	Enumerated	10415

Defined values:

— BEARER_RELEASED (0)

Used when the bearer has been deactivated as a result from normal signalling handling.

— INSUFFICIENT_SERVER_RESOURCES (1)

The server is overloaded and needs to end the session.



— INSUFFICIENT_BEARER_RESOURCES (2)

Used when the bearer has been deactivated because of insufficient bearer resources at a transport gateway.

5.2.2.16 AF-Application-Identifier

The AF-Application-Identifier AVP, see Table 37, is of type `OctetString`, and it contains information that identifies the particular service that the Rx service session belongs to.

Table 37 AF-Application-Identifier AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	504	12	OctetString	10415

Example

```
+g.poc.talkburst
```

5.2.2.17 Codec-Data

The Codec-Data AVP, see Table 38, is of type `OctetString` and must contain codec-related information known at the P-CSCF.

Table 38 Codec-Data AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
1	1	0	524	>12	OctetString	10415

This information must be encoded as follows:

- The first line of the value of the Codec-Data AVP must consist of either the word “uplink” or the word “downlink”(in ASCII, without quotes, followed by a new-line character (CRLF). The semantics of these words are the following:
 - “uplink” indicates that the SDP was received from the UE and sent to the network.
 - “downlink” indicates that the SDP was received from the network and sent to the UE.
- The second line of the value of the Codec-Data AVP must consist of either the word “offer” or the word “answer”, or the word “description” in ASCII, without quotes, followed by a new-line character (CRLF). The semantics of these words are the following:



- “offer” indicates that SDP lines from an SDP offer according to [RFC 3264 An Offer/Answer Model with the Session Description Protocol \(SDP\)](#) are being provisioned in the Codec-Data AVP.
 - “answer” indicates that SDP lines from an SDP answer according to [RFC 3264 An Offer/Answer Model with the Session Description Protocol \(SDP\)](#) are being provisioned in the Codec-Data AVP.
 - “description” – not used.
- The rest of the value consists of SDP lines in ASCII encoding separated by new-line characters, as specified in [RFC2327 SDP: Session Description Protocol](#). The first of these lines is to be an “m” line. The remaining lines are to be any available SDP “a” and “b” lines related to that “m” line. However, to avoid duplication of information, the SDP “a=sendrecv”, “a=recvonly”, “a=sendonly”, “a=inactive”, “b:AS”, “b:RS”, and “b:RR” lines are not included.

ABNF definition:

```
Codec-Data = SDP-origin
            SDP-Type
            1*SDP-Information
            SDP-Origin = ("uplink" / "downlink") CRLF
            ; uplink – SDP received from the UE
            ; downlink – SDP sent to the UE
            SDP-Type = ("offer" / "answer" / "description") CRLF
            ; offer – SDP Offer according to RFC3264
            ; answer – SDP Answer according to RFC3264
            ; description – not used
            SDP-Information = media-field
                            *[ bandwidth-field ]
                            *[ attribute-field ]
            ; media-field as defined in reference [4]
            ; bandwidth-field as defined in reference [4]

            ; attribute-field as defined in reference [4]
```

Example

```
uplink
answer
m=audio 49230 RTP/AVP 96 97 98
a=rtpmap:96 L8/8000
a=rtpmap:97 L16/8000
a=rtpmap:98 L16/11025/2
```

5.2.2.18

Experimental-Result

The Experimental-Result AVP, see Table 39, is used to indicate whether a particular vendor-specific request was completed successfully or whether an error occurred.



Table 39 Experimental-Result AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
0	1	0	297	32	Grouped	10415

Grammar:

```
< Experimental-Result > ::= < AVP Header: 297 >  
    { Vendor-Id }  
    { Experimental-Result-Code }
```

5.2.2.19

Experimental-Result-Code

The Experimental-Result-Code AVP, see Table 40, contains a vendor-assigned value representing the result of processing the request. An AA-Answer (AAA) message can contain an Experimental-Result-Code AVP. When this AVP exists in a message then P-CSCF always treats it as a negative response and terminates the ongoing SIP service, unless the SIP Session Continue function is enabled.

Table 40 Experimental-Result-Code AVP

V	M	P	AVP Code	AVP Length	AVP Data Type	Vendor-ID
0	1	0	298	12	Unsigned32	10415



6 Security Considerations

6.1 IPsec Tunnel

The communication between the P-CSCF and the PCRF can be secured using IPsec (Zb interface) on the IP transport layer, refer to the [3GPP TS 33.210 3G security; Network Domain Security \(NDS\); IP network layer security](#) specification.

IP Security (IPsec) tunnels can be defined between the two nodes. Internet Key Exchange version 1 (IKEv1) performs mutual authentication between the two nodes and establishes an IKE Security Association that includes shared secret information used to establish IPsec Security Associations (SAs). Different forms of authentication and encryptions can be selected when defining the IPsec tunnels. For the native CSCF, refer to *Security Management User Guide*, and for the virtual CSCF, refer to *eVIP Management Guide*.





7 Related Standards

This section states the related standards and explains any deviations from them.

3GPP R7 is used as input.

TLS is not supported.