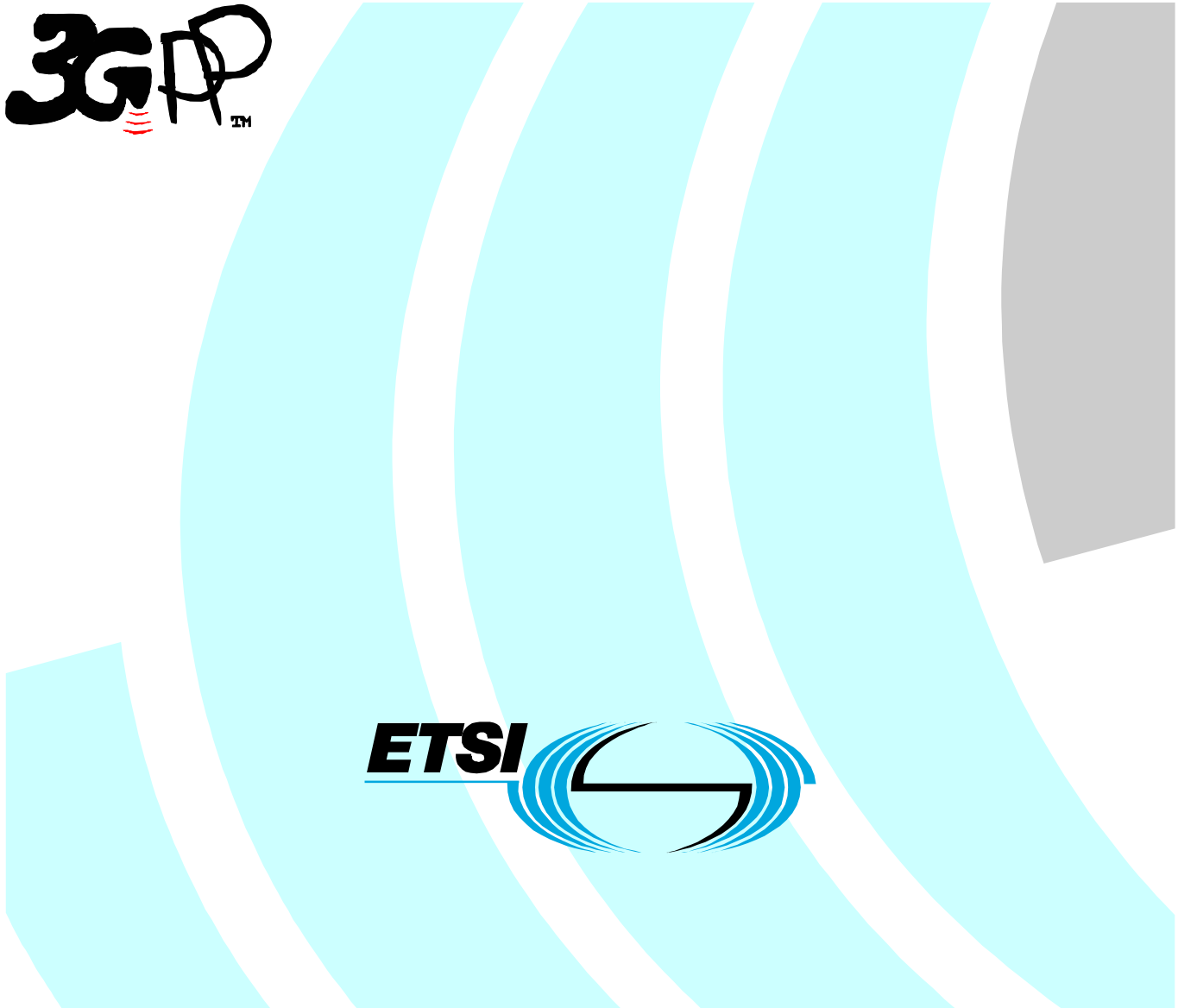
ETSI TS 129 209 V6.1.0 (2004-12)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
Policy control over Gq interface
(3GPP TS 29.209 version 6.1.0 Release 6)



Reference
DTS/TSGN-0329209v610

Keywords
UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp .

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document provides the stage 3 specification of the Gq interface. The functional requirements and the stage 2 specifications of the Gq interface are contained in 3GPP TS 23.002 [2] and 3GPP TS 23.207 [3]. The Gq interface is used for session based policy set-up information exchange between the Policy Decision Function (PDF) and the Application Function (AF).

Whenever it is possible the present document specifies the requirements for the protocol by reference to specifications produced by the IETF within the scope of Diameter. Where this is not possible, extensions to Diameter are defined within the present document.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 23.002: "Network architecture".

[3] 3GPP TS 23.207: "End-to-end Quality of Service (QoS) concept and architecture".

[4] 3GPP TS 29.207: "Policy control over Go interface".

[5] 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows".

[6] IETF RFC 3588: "Diameter Base Protocol".

[7] draft-ietf-aaa-diameter-nasreq-17.txt: "Diameter Network Access Server Application".

[8] IETF RFC 2234: "Augmented BNF for syntax specifications: ABNF".

[9] IETF RFC 3520: "Session Authorization Policy Element".

[10] 3GPP TS 33.210: "3G Security; Network Domain Security (NDS); IP network layer security".

[11] IETF RFC 3556: "Session Description Protocol (SDP) Bandwidth Modifiers for RTP Control Protocol (RTCP) Bandwidth".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply:

Application Function (AF): element offering applications that require the control of IP bearer resources.

NOTE: The AF is capable of communicating with the PDF to transfer dynamic QoS-related application information. One example of an AF is the P-CSCF of the IM CN subsystem.

AF session: established by an application level signalling protocol offered by the AF that requires a session set-up with explicit session description before the use of the service

NOTE: One example of an application session is an IMS session.

AF session signalling: used to control the AF session

NOTE: One example of AF session signalling is SIP/SDP.

Attribute-Value Pair (AVP): See RFC 3588 [6], corresponds to an Information Element in a Diameter message.

3.2 Abbreviations

For the purpose of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply:

AAA	AA-Answer
AAR	AA-Request
AF	Application Function
ASA	Abort-Session-Answer
ASR	Abort-Session-Request
AVP	Attribute-Value Pair
GCID	GPRS Charging ID
IANA	Internet Assigned Numbers Authority
NASREQ	Network Access Server Application
P-CSCF	Proxy - Call Session Control Function
PDF	Policy Decision Function
RAA	Re-Auth-Answer
RAR	Re-Auth-Request
SBLP	Service Based Local Policy
SDI	Session Description Information
STA	Session-Termination-Answer
STR	Session-Termination-Request

4 Gq interface

4.1 Overview

The Gq interface is used for the service-based policy set-up information exchange between the PDF and the AF, e.g. the P-CSCF. As defined in the stage 2 specifications (3GPP TS 23.207 [3]), this information is used by the PDF for the Service Based Local Policy (SBLP) decisions. The PDF exchanges the policy information with the GGSN as specified in 3GPP TS 29.207 [4].

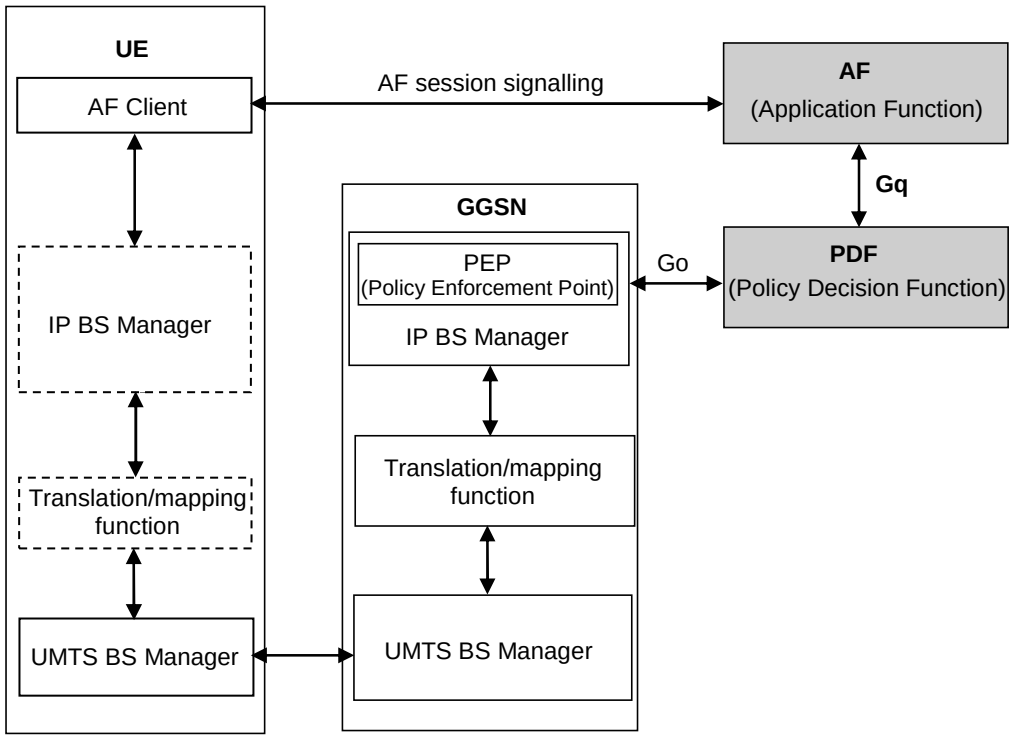
The Gq interface may be an intra- or inter-domain interface. One PDF shall be able to serve more than one AF and one given AF may interact with a number of PDFs, although on an AF session basis, it shall interact with only a single PDF.

Signalling flows related to the Gq interface are specified in 3GPP TS 29.208 [5].

4.2 Gq reference model

The Gq interface is defined between the PDF and the AF. The Gq interface may be an intra- or inter-domain interface. The PDF is in the same PLMN as the GGSN.

The relationships between the different functional entities involved are depicted in figure 4.1.



NOTE: For clarity in the diagram, the network elements that are not involved in SBLP are not presented here (e.g. radio network elements, SGSN, etc).

Figure 4.1: Gq interface architecture model

4.3 Functional elements and capabilities

4.3.1 Policy Decision Function (PDF)

The PDF acts as a Policy Decision Point for service based local policy control. The PDF makes the policy decisions based on the session and media related information obtained from the AF via the Gq interface. The PDF shall exchange the decision information with the GGSN via the Go interface.

4.3.2 Application Function (AF)

The AF is an element offering applications that require the control of IP bearer resources (e.g. UMTS PS domain/GPRS domain resources). One example of an application function is the P-CSCF. The AF shall use the Gq interface to exchange service based policy information with the PDF.

5 Policy control procedures

5.1 PDF

5.1.1 Initial authorization of QoS resources

When receiving an initial AA-Request from the AF, the PDF allocates Authorization-Token. The PDF shall store the Diameter base protocol Session-Id received in the AA-Request message for the Authorization-Token. If the AA-Request contains the Media-Component-Description Attribute-Value Pair(s) (AVP(s)) the PDF shall authorize the required QoS resources and store the SBLP for the session based on the service information. If the AA-Request contains Flow-Grouping AVP(s), the PDF shall only authorize the QoS if the IP flows are distributed to PDP contexts in a way that is allowed by the Flow-Grouping AVP(s). The PDF sends the allocated token in the Authorization-Token AVP to the AF in the AA-Answer message.

5.1.2 Resource reservation

When receiving a bearer authorization request from the Go interface, the PDF shall authorize the request according to the stored SBLP for the session, if available.

For a bearer authorization request with a new authorization token the PDF shall behave as described within the present paragraph: If the SBLP is not available for the session, or if the AF has instructed the PDF to do so, the PDF shall send the Re-Auth_Request message with the SERVICE_INFORMATION_REQUEST indication in the Specific-Action AVP to the AF to request the service information. When receiving the Media-Component-Description AVP(s) in the Re-Auth-Answer message, the PDF shall authorize the required QoS resources and shall store the SBLP for the session. If SBLP is available for the session butauthorization for unknown flow identifiers is being requested, and the AF has not instructed the PDF to contact it at bearer authorization, the PDF shall deny the authorization without contacting the AF.

For a bearer authorization request for an authorization token already authorized by the PDF, the PDF shall behave as described within the present paragraph: If the request contains binding information for media with no corresponding SBLP available at the PDF, or if the PDF has already authorized the same binding information and not obtained updated service information since then, or if the AF has instructed the PDF to do so, the PDF shall send a Re-Auth-Request message with the SERVICE_INFORMATION_REQUEST indication in the Specific-Action AVP to the AF to request updated service information. When receiving the Media-Component-Description AVP(s) in the Re-Auth-Answer message the PDF shall authorize the required QoS resources and shall store the SBLP for the session.

After the bearer authorization the PDF shall send possible new access network charging identifier(s) (e.g. GCID), received from the GGSN during the bearer authorization to the AF for charging correlation purposes, and an access network charging-address (e.g. GGSN IP Address), if the AF has instructed the PDF to do so. The PDF does this by sending the Re-Auth_Request message with the CHARGING_CORRELATION_EXCHANGE indication in the Specific-Action AVP to the AF.

5.1.3 Gate function

The AF shall indicate to the PDF as part of the Media-Component-Description AVP(s) whether the media IP flow(s) should be enabled or disabled at the bearer authorization. The PDF may receive a separate AA-Request message(s) from the AF to enable or disable specified IP flows. The PDF shall reply with an AA-Answer and shall include the Access-Network-Charging-Identifier(s) available at this moment. The PDF makes the final decision to enable or disable the authorized IP flows.

5.1.4 Session modification

The PDF may receive the AA-Request message from the AF with modified service information. The PDF shall store the SBLP for the session based on the new service information. The PDF shall acknowledge the session modification by issuing an AA-Answer back to the AF and shall include the Access-Network-Charging-Identifier(s) and may include the Access-Network-Charging-Address, if they are available at this moment and have not yet been supplied earlier to the AF. The PDF shall enforce corresponding bearer modifications as detailed in 3GPP TS 29.207 [4].

5.1.5 Bearer modification

The bearer authorization for the session- or bearer-initiated modification is performed as specified in 3GPP TS 29.207 [4].

If the AF has requested a notification at the loss of a bearer, and the PDF receives a notification that a PDP context is modified to the bandwidth of 0 kbit via the Go interface, the PDF shall send a Re-Auth_Request with the value for the Specific-Action AVP set to INDICATION_OF_LOSS_OF_BEARER and shall indicate the affected IP flows with the Flows AVP(s) if not all IP flows within an AF session are affected.

If the AF has requested a notification at the recovery of a bearer, and the PDF receives a notification that a PDP context is modified from the bandwidth of 0 kbit to a higher value via the Go interface, the PDF shall send a Re-Auth_Request with the value for the Specific-Action AVP set to INDICATION_OF_RECOVERY_OF_BEARER and shall indicate the affected IP flows with the Flows AVP(s) if not all IP flows within an AF session are affected.

5.1.6 Revoke authorization

When receiving the Session-Termination-Request message from the AF, the PDF shall revoke the bearer authorization as detailed in 3GPP TS 29.207 [4].

5.1.7 Indication of bearer release

If the AF has requested a notification at the release of a bearer, and the PDF receives a notification that a PDP context is released via the Go interface, but not all IP flows within the corresponding AF session are affected by the PDP context release, the PDF shall send a Re-Auth_Request with the value for the Specific-Action AVP set to INDICATION_OF_RELEASE_OF_BEARER and shall indicate the affected IP flows with the Flows AVP(s) and the appropriate Abort-Cause AVP value.

When the GGSN informs the PDF of the PDP context release and all IP flows within the corresponding AF session are affected, the PDF shall inform the AF about this event by sending the Abort-Session-Request message with the appropriate Abort-Cause AVP value.

5.2 AF

5.2.1 Initial authorization of QoS resources

When receiving an AF session signalling message initiating a new AF session, the AF shall request an authorization for the session from the PDF by sending the AA-Request message. The AF shall include the corresponding Media-Component-Description AVP(s) into the message if the SDI is already available at the AF. The AF may include the Flow-Grouping AVP(s) to request a particular way on how the IP flows described within the service description are distributed to PDP contexts. The AF may also include the AF-Charging-Identifier AVP into the message for the charging correlation purposes.

The AF receives the Authorization-Token AVP from the PDF in the AA-Answer message. The usage of Authorization-Token is application dependent.

5.2.2 Resource reservation

The PDF may contact the AF at the UE resource reservation by sending the Re-Auth-Request message with a request for the service information. The AF shall respond with the Re-Auth-Answer message containing the Media-Component-Description AVP(s). The information in the Media-Component-Description AVP(s) may be based on the session description information negotiated within the AF session signalling. The AF does not need to send a new authorization request back to the PDF when receiving a Re-Auth-Request message with a request for the service information. The AF may include the Flow-Grouping AVP(s) to request a particular way on how the IP flows described within the service description are distributed to PDP contexts.

The AF may receive an access network charging identifier (e.g. GCID) and access network charging address (e.g. GGSN IP address) for charging correlation purposes from the PDF in a separate Re-Auth-Request message after the bearer has been authorized. The AF does not need to send a new authorization request when receiving a Re-Auth-

Request message with access network charging identifier (e.g. GCID) and access network charging address (e.g. GGSN IP address).

5.2.3 Gate function

The AF shall indicate to the PDF as part of the Media-Component-Description whether the media IP flow(s) should be enabled or disabled at the bearer authorization. Depending on the application, the AF may instruct the PDF also during the session when the IP flow(s) are to be enabled or disabled to pass through the access network. The AF does this by sending the AA-Request message containing the Media-Component- Description AVP(s) that contains the flow status information for the flows to be enabled or disabled.

5.2.4 Session modification

During the AF session modification, the AF shall send an update for the session description information to the PDF based on the new SDI exchanged within the AF session signalling. The AF does this by sending the AA-Request message containing the Media-Component-Description AVP(s) containing the updated service information. The AF may include the Flow-Grouping AVP(s) to request a particular way on how the IP flows described within the service description are distributed to PDP contexts.

5.2.5 Revoke authorization

When AF session is terminated the AF shall revoke the corresponding bearer authorization by the sending Session-Termination-Request message to the PDF.

5.3 IMS related P-CSCF procedures

5.3.1 Provisioning of Service Information at P-CSCF

The P-CSCF shall send service information to the PDF upon every SIP message that includes an SDP answer payload. The service information shall be derived both from the SDP offer and the SDP answer. This ensures that the PDF receives proper information to perform media authorization for all possible IMS session set-up scenarios, and that the PDF is also capable of handling session modifications.

All media components in the SDP shall be authorized. Therefore, the P-CSCF shall derive a media component within the session information from every SDP media component, as detailed in 3GPP TS 29.208 [5]. The SDP contains sufficient information about the session, such as the end-points' IP address and port numbers and bandwidth requirements.

The P-CSCF shall derive Flow-Description AVP within the service information from the SDP as follows:

- An uplink Flow-Description AVP shall be formed as follows: The destination address and port number shall be taken from the connection information parameter of the SDP sent by the P-CSCF in downlink direction, while the source IP address may be formed from the address present in the SDP received by the P-CSCF in uplink direction (taking into account only the 64 bit prefix of the IPv6 address), and the source port number shall be wildcarded. For example, assuming UE A sends an SDP to UE B, the PDF of UE B uses the address present in this SDP for the destination address of UE B's uplink Flow-Description AVP, while the PDF of the UE A uses the 64 bit prefix of the same address for the source address of UE A's uplink Flow-Description AVP. If the source address is not formed from the 64 bit prefix, the source address shall be wildcarded.

- An downlink Flow-Description AVP shall be formed as follows: The destination address and port number shall be taken from the connection information parameter of the SDP received by the P-CSCF in uplink direction, while the source IP address may be formed (in order to reduce the possibilities of bearer misuse) from the destination address in the SDP sent by the P-CSCF in downlink direction (taking into account only the 64 bit prefix of the IPv6 address) and the source port number shall be wildcarded. For example, assuming UE A sends an SDP to UE B, the PDF of UE a uses the address present in this SDP for the destination address of UE A's downlink Flow-Description AVP, while the PDF of UE B uses the 64 bit prefix of the same address for the source address of UE B's downlink Flow-Description AVP. If the source address is not formed from the 64 bit prefix, the source address shall be wildcarded.

The P-CSCF shall derive the bandwidth information within the service information, from the "b=AS" SDP parameter, as detailed in 3GPP TS 29.208 [5]. For the possibly associated RTCP IP flows, the P-CSCF shall use the SDP "b=RR" and "b=RS" parameters, if present, as specified in 3GPP TS 29.208 [5]. The "b=AS", "b=RR" and "b=RS" parameters in the SDP contain all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTCP payload, or IP, UDP and RTCP.

5.3.2 Enabling of IP Flows at P-CSCF

Prior to the completion of the SIP session set-up, i.e. until the 200 OK(INVITE) is received, the P-CSCF may enable or disable media IP flows depending on operator policy, thus allowing of forbidding early media in forward and/or backward direction. Only to disable early media, the P-CSCF may modify the values of the Flow-Status AVPs derived from SDP according to 3GPP TS 29.208 [5]. If the P-CSCF chooses to modify the values, the P-CSCF shall store the last received SDP.

When the 200 OK is received, the P-CSCF shall enable all media IP flows according to the direction attribute within the last received SDP, as specified in 3GPP TS 29.208 [5]. When the 200 OK is received and the P-CSCF previously provided modified values of the Flow-Status AVPs in the session information, the P-CSCF shall provide service information with values of the Flow-Status AVPs corresponding to the last received SDP.

If the P-CSCF receives SDP answers after the completion of the SIP session set-up, i.e. after the 200 OK(INVITE) is received, the P-CSCF shall provide the Flow-Status AVPs as derived from the SDP according to 3GPP TS 29.208 [5].

6 Gq protocol

6.1 Protocol support

The Diameter Base Protocol as specified in RFC 3588 [6] shall apply except as modified by the defined Gq application specific procedures and AVPs. Unless otherwise specified, the procedures (including error handling and unrecognized information handling) are unmodified.

In addition to the AVPs defined within the clause 6.5, the Diameter AVPs from the Diameter base application (RFC 3588 [6]) are reused within the Diameter messages of the Gq application. The support of AVPs from the Diameter Network Access Server Application (NASREQ) (draft-ietf-aaa-diameter-nasreq-17 [7]) is not required from Diameter implementations that conform to the present document.

Accounting functionality (Accounting Session State Machine, related command codes and AVPs) is not used in the Gq interface.

The Gq application is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

Editor's note: The application id needs to be allocated from IANA. With regard to the Diameter protocol defined over the Gq interface, the PDF acts as a Diameter server, in the sense that it is the network element that handles authorization requests for a particular realm. The AF acts as the Diameter Client, in the sense that is the network element requesting authorization to use bearer path network resources.

The support of Diameter agents between the PDF and the AF, is optional for the IMS, where the Gq is intra operator i.e. GGSN, PDF and P-CSCF are all in the same network.

6.1.1 Advertising application support

The AF and the PDF shall advertise the support of the Gq specific Application by including the value of the application identifier in the Auth-Application-Id AVP and the value of the 3GPP (10415) in the 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.

6.2 Securing Diameter messages

For secure transport of Diameter messages, see 3GPP TS 33.210 [10].

6.3 Gq messages

Existing Diameter command codes from the Diameter base protocol RFC 2588 [6] and the NASREQ Diameter application (draft-ietf-aaa-diameter-nasreq-17 [7]) are used with the Gq specific AVPs. A Gq specific Auth-Application id is used together with the command code to identify the Gq messages.

NOTE: The notion of NAS (Network Access Server) is not used here, NASREQ is just used for protocol purposes, not for its functional meaning.

6.3.1 AA-Request (AAR) command

The AAR command, indicated by the Command-Code field set to 265 and the 'R' bit set in the Command Flags field, is sent by an AF to the PDF in order to request the authorization for the bearer usage for the AF session.

Message Format:

```
<AA-Request> ::= < Diameter Header: 265, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                *[ Media-Component-Description ]
                *[ Flow-Grouping ]
                 [ AF-Charging-Identifier ]
                 [ SIP-Forking-Indication ]
                *[ Gq-Specific-Action ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

6.3.2 AA-Answer (AAA) command

The AAA command, indicated by the Command-Code field set to 265 and the 'R' bit cleared in the Command Flags field, is sent by the PDF to the AF in response to the AAR command.

Message Format:

```
<AA-Answer> ::=  < Diameter Header: 265, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 [ Authorization-Token ]
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ AVP ]
```

6.3.3 Re-Auth-Request (RAR) command

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PDF to the AF in order to indicate Gq specific action.

As an option, the AF may send an AAR command to the PDF to update the service information when receiving an RAA command. However, application-specific authentication and/or authorization messages are not mandated for the Gq application in response to an RAR command.

The values INDICATION_OF_LOSS_OF_BEARER, INDICATION_OF_RECOVERY_OF_BEARER and INDICATION_OF_RELEASE_OF_BEARER of the Gq-Specific-Action AVP shall not be combined with each other in an Re-Auth-Request.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                *{ Gq-Specific-Action }
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                *[ Flows ]
                 [ Abort-Cause ]
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

6.3.4 Re-Auth-Answer (RAA) command

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

Message Format:

```
<RA-Answer> ::=  < Diameter Header: 258, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                *[ Media-Component-Description ]
                *[ Flow-Grouping ]
                 [ Origin-State-Id ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ AVP ]
```

6.3.5 Session-Termination-Request (STR) command

The STR command, indicated by the Command-Code field set to 275 and the 'R' bit set in the Command Flags field, is sent by the AF to inform the PDF that an authorized session shall be terminated.

Message Format:

```
<ST-Request> ::= < Diameter Header: 275, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Auth-Application-Id }
                 { Termination-Cause }
                 [ Destination-Host ]
                *[ Class ]
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

6.3.6 Session-Termination-Answer (STA) command

The STA command, indicated by the Command-Code field set to 275 and the 'R' bit cleared in the Command Flags field, is sent by the PDF to the AF in response to the STR command.

Message Format:

```
<ST-Answer>  ::= < Diameter Header: 275, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Auth-Application-Id }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                 [ Origin-State-Id ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ Proxy-Info ]
                 [ AVP ]
```

6.3.7 Abort-Session-Request (ASR) command

The ASR command, indicated by the Command-Code field set to 274 and the 'R' bit set in the Command Flags field, is sent by the PDF to inform the AF that all bearer resources for the authorized session have become unavailable.

Message Format:

```
<AS-Request>  ::= < Diameter Header: 274, REQ, PXY >
                  < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                 { Abort-Cause }
                 [ Origin-State-Id ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                 [ AVP ]
```

6.3.8 Abort-Session-Answer (ASA) command

The ASA command, indicated by the Command-Code field set to 274 and the 'R' bit cleared in the Command Flags field, is sent by the AF to the PDF in response to the ASR command.

Message Format:

```
<AS-Answer>  ::=  < Diameter Header: 274, PXY >
                  < Session-Id >
                  { Origin-Host }
                  { Origin-Realm }
                  [ Result-Code ]
                  [ Experimental-Result ]
                  [ Origin-State-Id ]
                  [ Error-Message ]
                  [ Error-Reporting-Host ]
                 *[ Failed-AVP ]
                 *[ Redirected-Host ]
                  [ Redirected-Host-Usage ]
                  [ Redirected-Max-Cache-Time ]
                 *[ Proxy-Info ]
                 *[ AVP ]
```

6.4 Experimental-Result-Code AVP values

This subclause defines the specific values of the Experimental-Result-Code AVP:

INVALID_SERVICE_INFORMATION (5061)

The service information provided by the AF is invalid or insufficient for the server to perform the requested action.

FILTER_RESTRICTIONS (5062)

The Flow_Description AVP(s) cannot be handled by the server because restrictions defined in clause 6.5.8 are not observed.

6.5 Gq specific AVPs

Table 6.5.1 describes the Diameter AVPs defined for the Gq interface protocol, their AVP Code values, types, possible flag values and whether or not the AVP may be encrypted. The Vendor-Id header of all AVPs defined in the present document shall be set to 3GPP (10415).

Table 6.5.1: Gq specific Diameter AVPs

				AVP Flag rules (note 1)				
Attribute Name	**AVP Code**	**Clause defined**	**Value Type (note 2)**	**Must**	**May**	**Should not**	**Must not**	**May Encr.**
Abort-Cause	500	6.5.1	Enumerated	M,V	P			Y
Access-Network-Charging-Address	501	6.5.2	Address	M,V	P			Y
Access-Network-Charging-Identifier	502	6.5.3	Grouped	M,V	P			Y
Access-Network-Charging-Identifier-Value	503	6.5.4	OctetString	M,V	P			Y
AF-Application-Identifier	504	6.5.5	OctetString	M,V	P			Y
AF-Charging-Identifier	505	6.5.6	OctetString	M,V	P			Y
Authorization-Token	506	6.5.7	OctetString	M,V	P			Y
Flow-Description	507	6.5.8	IPFilterRule	M,V	P			Y
Flow-Grouping	508	6.5.9	Grouped	M,V	P			Y
Flow-Number	509	6.5.10	Unsigned32	M,V	P			Y
Flows	510	6.5.11	Grouped	M,V	P			Y
Flow-Status	511	6.5.12	Enumerated	M,V	P			Y
Flow-Usage	512	6.5.13	Enumerated	M,V	P			Y
Specific-Action	513	6.5.14	Enumerated	M,V	P			Y
Max-Requested-Bandwidth-DL	515	6.5.16	Unsigned32	M,V	P			Y
Max-Requested-Bandwidth-UL	516	6.5.17	Unsigned32	M,V	P			Y
Media-Component-Description	517	6.5.18	Grouped	M,V	P			Y
Media-Component-Number	518	6.5.19	Unsigned32	M,V	P			Y
Media-Sub-Component AVP	519	6.5.20	Grouped	M,V	P			Y
Media-Type	520	6.5.21	Enumerated	M,V	P			Y
RR-Bandwidth	521	6.5.22	Unsigned32	M,V	P			Y
RS-Bandwidth	522	6.5.23	Unsigned32	M,V	P			Y
SIP-Forking-Indication	523	6.5.24	Enumerated	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 [6].
NOTE 2: The value types are defined in RFC 3588 [6].

6.5.1 Abort-Cause AVP

The Session-Abort-Cause AVP (AVP code 500) is of type Enumerated, and determines the cause of a session abort request or of an RAR indicating a PDP context release. The following values are defined:

BEARER_RELEASED (0)

This value is used when the bearer has been deactivated as a result from normal signalling handling. For GPRS the bearer refers to the PDP Context.

INSUFFICIENT_SERVER_RESOURCES (1)

This value is used to indicate that the server is overloaded and needs to abort the session.

INSUFFICIENT_BEARER_RESOURCES (2)

This value is used when the bearer has been deactivated due to insufficient bearer resources at a transport gateway (e.g. GGSN for GPRS).

6.5.2 Access-Network-Charging-Address AVP

The Access-Network-Charging-Address AVP (AVP code 501) is of type Address, and it indicates the IP Address of the network entity within the access network performing charging (e.g. the GGSN IP address). The Access-Network-Charging-Address AVP should not be forwarded over an inter-operator interface.

6.5.3 Access-Network-Charging-Identifier AVP

The Access-Network-Charging-Identifier AVP (AVP code 502) is of type Grouped, and contains a charging identifier (e.g. GCID) within the Access-Network-Charging-Identifier-Value AVP along with information about the flows transported within the corresponding bearer within the Flows AVP. If no Flows AVP is provided, the Access-Network-Charging-Identifier-Value applies for all flows within the AF session.

The Access-Network-Charging-Identifier AVP can be sent from the PDF to the AF. The AF may use this information for charging correlation with session layer.

AVP Format:

```
Access-Network-Charging-Identifier ::= < AVP Header: x >
                    { Access-Network-Charging-Identifier-Value}
                    *[ Flows ]
```

6.5.4 Access-Network-Charging-Identifier-Value AVP

The Access-Network-Charging-Identifier-Value AVP (AVP code 503) is of type OctetString, and contains a charging identifier (e.g. GCID).

6.5.5 AF-Application-Identifier AVP

The AF-Application-identifier AVP (AVP code 504) is of type OctetString, and it contains information that identifies the particular service that the AF service session belongs to. This information may be used by the PDF to differentiate QoS for different application services. For example the AF-Application-Identifier may be used as additional information together with the Media-Type AVP when the QoS class for the bearer authorization at the Go interface is selected. The AF-Application-Identifier may be used also to complete the QoS authorization with application specific default settings in the PDF if the AF does not provide full Session-Component-Description information.

6.5.6 AF-Charging-Identifier AVP

The AF-Charging-Identifier AVP (AVP code 505) is of type OctetString, contains the AF Charging Identifier that is sent by the AF. This information may be used for charging correlation with bearer layer.

6.5.7 Authorization-Token AVP

The Authorization-Token AVP (AVP code 506) is of type OctetString, and contains the Authorization Token defined in the RFC 3520 [9].

6.5.8 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).
- Source and destination IP address (possibly masked).
- Protocol.
- Source and destination port (list or ranges).

The IPFilterRule type shall be used with the following restrictions:

- Only the Action "permit" shall be used.
- No "options" shall be used.
- The invert modifier "!" for addresses shall not be used.
- The keyword "assigned" shall not be used.

If any of these restrictions is not observed by the AF, the server shall send an error response to the AF containing the Experimental-Result-Code AVP with value FILTER_RESTRICTIONS.

The Flow description AVP shall 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.

6.5.9 Flow-Grouping AVP

The Flow-Grouping AVP (AVP code 508) is of type Grouped, and it indicates that no other IP Flows shall be transported together with the listed IP Flows in the same PDP context(s).

If Flow-Grouping AVP(s) have been provided in earlier service information, but are not provided in subsequent service information, the old flow grouping remains valid.

If Flow-Grouping AVP(s) have been provided in earlier service information, and new Flow-Grouping AVP(s) are provided, the new flow grouping information replaces the previous information. Previous flow grouping information is invalidated even if the new Flow-Grouping AVP(s) affect other IP flows.

A Flow-Grouping AVP containing no Flows AVP may be used to invalidate flow grouping information provided in earlier service information. A Flow-Grouping AVP containing no Flows AVP shall not be supplied together with other Flow-Grouping AVP(s).

If earlier service information has already been provided, flow grouping information in subsequent service information shall not restrict the flow grouping further for IP flows already described in the previous service information. However, new IP flows described for the first time in the subsequent service information may be added to existing flow groups or in new flow groups.

AVP Format:

```
Flow-Grouping ::= < AVP Header: x >
        *[Flows]
```

6.5.10 Flow-Number AVP

The Flow-Number AVP (AVP code 509) is of type Unsigned32, and it contains the ordinal number of the IP flow(s), assigned according to the rules in annex C of 3GPP TS 29.207 [4].

6.5.11 Flows AVP

The Flows AVP (AVP code 510) is of type Grouped, and it indicates IP flows via their flow identifiers.

If no Flow-Number AVP(s) are supplied, the Flows AVP refers to all Flows matching the media component number.

AVP Format:

```
Flows::= < AVP Header: x >
      { Media-Component-Number}
      *[ Flow-Number]
```

6.5.12 Flow-Status AVP

The Flow-Status AVP (AVP code 511) is of type Enumerated, and describes whether the IP flow(s) are enabled or disabled. The following values are defined:

ENABLED-UPLINK (0)

This value shall be used to enable associated uplink IP flow(s) and to disable associated downlink IP flow(s). If any downlink RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.

ENABLED-DOWNLINK (1)

This value shall be used to enable associated downlink IP flow(s) and to disable associated uplink IP flow(s). If any uplink RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.

ENABLED (2)

This value shall be used to enable all associated IP flow(s) in both directions.

DISABLED (3)

This value shall be used to disable all associated IP flow(s) in both directions. If any RTCP IP flow(s) are identified by the Flow_Usage AVP(s), those flow(s) shall be enabled.

REMOVED (4)

This value shall be used to remove all associated IP flow(s). The IP Filters for the associated IP flow(s) shall be removed. The associated IP flows shall not be taken into account when deriving the authorized QoS.

6.5.13 Flow-Usage AVP

The Flow-Usage AVP (AVP code 512) is of type Enumerated, and provides information about the usage of IP Flows. The following values are defined:

NO_INFORMATION (0)

This value is used to indicate that no information about the usage of the IP flow is being provided

RTCP (1)

This value is used to indicate that an IP flow is used to transport RTCP.

NO_INFORMATION is the default value.

NOTE: An AF may choose not to identify RTCP flows, e.g. in order to avoid that RTCP flows are always enabled by theserver.

6.5.14 Specific-Action AVP

The Specific-Action AVP (AVP code 513) is of type Enumerated.

Within a PDF initiated Re-Authorization Request, the Gq-Specific-Action AVP determines the type of the action.

Within an initial AA request the AF may use the Specific-Action AVP to request specific actions from the server at the bearer events and to limit the contact to such bearer events where specific action is required. If the Specific-Action AVP is omitted within the initial AA request, no notification of any of the events defined below is requested.

The following values are defined:

SERVICE_INFORMATION_REQUEST (0)

Within a RAR, this value shall be used when the server requests the service information from the AF for the bearer event. In the AAR, this value indicates that the AF requests the server to demand service information at each bearer authorization.

CHARGING_CORRELATION_EXCHANGE (1)

Within a RAR, this value shall be used when the server reports the access network charging identifier to the AF. The Access-Network-Charging-Identifier AVP shall be included within the request. In the AAR, this value indicates that the AF requests the server to provide an access network charging identifier to the AF at each bearerestablishment/modification, when a new access network charging identifier becomes available.

INDICATION_OF_LOSS_OF_BEARER (2)

Within a RAR, this value shall be used when the server reports a loss of a bearer (e.g. in the case of GPRS PDP context bandwidth modification to 0 kbit) to the AF. In the AAR, this value indicates that the AF requests the server to provide a notification at the loss of a bearer.

INDICATION_OF_RECOVERY_OF_BEARER (3)

Within a RAR, this value shall be used when the server reports a recovery of a bearer (e.g. in the case of GPRS, PDP context bandwidth modification from 0 kbit to another value) to the AF. In the AAR, this value indicates that the AF requests the server to provide a notification at the recovery of a bearer.

INDICATION_OF_RELEASE_OF_BEARER (4)

Within a RAR, this value shall be used when the server reports the release of a bearer (e.g. PDP context removal for GPRS) to the AF. In the AAR, this value indicates that the AF requests the server to provide a notification at the removal of a bearer.

6.5.15 Void

6.5.16 Max-Requested-Bandwidth-DL AVP

The Max-Requested-Bandwidth-DL AVP (AVP code 515) is of type Unsigned32, and it 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, e.g. IP, UDP, RTP and RTP payload.

6.5.17 Max-Requested-Bandwidth-UL AVP

The Max -Bandwidth-UL AVP (AVP code 516) is of type Unsigned32, and it 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, e.g. IP, UDP, RTP and RTP payload.

6.5.18 Media-Component-Description AVP

The Media-Component-Description AVP (AVP code 517) is of type Grouped, and it contains service information for a single media component within an AF session. It may be based on the SDI exchanged between the AF and the AF client in the UE. The information may be used by the server to determine authorized QoS and IP flow classifiers for bearer authorization and charging rule selection.

Within one Diameter message, a single IP flow shall 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 AVP(s).

If a Media-Component-Description AVP is not supplied, or if optional AVP(s) 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 flow(s) remains valid.

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

AVP format:

```
Media-Component-Description ::= < AVP Header: ?>
                                 { Media-Component-Number } ; Ordinal number of the media comp.
                                *[ Media-Sub-Component ]        ; Set of flows for one flow identifier
                                 [ AF-Application-Identifier ]
                                 [ Media-Type ]

                                 [ Max-Requested-Bandwidth-UL ]
                                 [ Max-Requested-Bandwidth-DL ]
                                 [ Flow-Status ]
                                 [ RS-Bandwidth ]
                                 [ RR-Bandwidth ]
```

6.5.19 Media-Component-Number AVP

The Media-Component-Number AVP (AVP code 518) is of type Unsigned32, and it contains the ordinal number of the media component, assigned according to the rules in annex C of 3GPP TS 29.207 [4].

6.5.20 Media-Sub-Component AVP

The Media-Sub-Component AVP (AVP code 519) is of type Grouped, and 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 3GPP TS 29.207 [4].

Possible Bandwidth information and Flow-Status information provided within the Media-Sub-Component AVP takes precedence over information within the encapsulating Media Component Description AVP. If a Media-Sub-Component- AVP is not supplied, or if optional AVP(s) 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 flow(s) remains valid, unless new information is provided within the encapsulating Media-Component-Description AVP. If Flow-Description AVP(s) are supplied, they replace all previous Flow-Description AVP(s), 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 may delete corresponding filters and state information.

AVP format:

```
Media-Sub-Component ::= < AVP Header: ?>
                         { Flow-Number }      ; Ordinal number of the IP flow
                       0*2[ Flow-Description ]        ; UL and/or DL
                         [ Flow-Status ]
                         [ Flow-Usage ]
                         [ Max-Requested-Bandwidth-UL ]
                         [ Max-Requested-Bandwidth-DL ]
```

6.5.21 Media-Type AVP

The Media-Type AVP (AVP code 520) is of type Enumerated, and it determines the media type of a session component. The following values are defined:

AUDIO (0)

VIDEO (1)

DATA (2)

APPLICATION (3)

CONTROL (4)

6.5.22 RR-Bandwidth AVP

The RR-Bandwidth AVP (AVP code 521) is of type Unsigned32, and it indicates the maximum required bandwidth in bits per second for RTCP receiver reports within the session component, as specified in RFC 3556 [11]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP.

6.5.23 RS-Bandwidth AVP

The RS-Bandwidth AVP (AVP code 522) is of type Unsigned32, and it indicates the maximum required bandwidth in bits per second for RTCP sender reports within the session component, as specified in RFC 3556 [11]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP.

6.5.24 SIP-Forking-Indication AVP

The SIP_Forking AVP (AVP code 523) is of type Enumerated, and describes if several SIP dialogues are related to one Diameter session.:

SINGLE_DIALOGUE (0)

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

SEVERAL_DIALOGUES (1)

This value is used to indicate that the Diameter session relates to several SIP dialogues.

Annex A (normative): Support for SIP forking

A.1 Support for SIP forking

The P-CSCF shall be able to handle forking when SBLP is applied. Forking can occur as specified in 3GPP TS 23.228 [4]. The related UE procedures are described in 3GPP TS 24.229 [14].

A.1.1 Authorization of resources for early media for forked responses

When a SIP session has been originated by a connected UE, the P-CSCF may receive multiple provisional responses due to forking before the first final answer is received. The P-CSCF shall apply the same authorization token to all the forked responses and the corresponding early dialogues.

The UE and the P-CSCF become aware of the forking only when the second provisional response arrives. For this, and any subsequent provisional response, the P-CSCF shall use an AA request within the existing Diameter session containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES and include the service information derived from the latest provisional response.

When receiving an AA request containing the SIP-Forking-Indication AVP with value SEVERAL_DIALOGUES, the PDF shall identify the existing authorization information for that Diameter session. The PDF shall authorize any additional media components and any increased QoS requirements for the previously authorized media components, as requested within the service information. The PDF shall authorize the maximum bandwidth required by any of the dialogues, but not the sum of the bandwidths required by all dialogues. Thus, the QoS authorized for a media component is equal to the highest QoS requested for that media component by any of the forked responses. The PDF shall also send additional packet classifiers as required by the Flow Description AVPs within the session information to the GGSN.

A.1.2 Updating the authorization information at the final answer

The P-CSCF shall store the SDP information for each early dialogue separately till the first final SIP answer is received. Then the related early dialogue is progressed to an established dialogue to establish the final SIP session. All the other early dialogues are terminated. The authorization information for the SIP session is updated to match the requirements of the remaining early dialogue only.

When receiving the first final SIP response, the P-CSCF shall send an AA request without the SIP-Forking-Indication AVP and include the service information derived from the SDP corresponding to the dialogue of the final response.

When receiving an AA request with no SIP-Forking-Indication AVP or with a SIP-Forking-Indication AVP with value SINGLE_DIALOGUE, the PDF shall. update authorization information and packet classifiers to match only the requirements of the service information within this AA request.

Annex B (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2004-09	25	NP-040421			Approved at CN Plenary and placed under change control	2.0.2	6.0.0
2004-12	26	NP-040586	001	1	Gmb. New AVP to indicate Multicast or Broadcast service	6.0.0	6.1.0
2004-12	26	NP-040586	002	1	Gmb. Table with reused AVPs	6.0.0	6.1.0
2004-12	26	NP-040586	003	1	Gmb. Correction to the Result-Code AVP	6.0.0	6.1.0
2004-12	26	NP-040586	009	1	Gmb. Correction to the Result-Code AVP	6.0.0	6.1.0
2004-12	26	NP-040586	008	3	Gmb. Update of AVPs codes and permanent failures codes.	6.0.0	6.1.0
2004-12	26	NP-040586	010		Gmb. Serving Network identity	6.0.0	6.1.0

History

Document history		
V6.1.0	December 2004	Publication