# All-IP Core Network Multimedia Domain

## Service Based Bearer Control – Tx Interface Stage 3

## Contents

1. Introduction ........................................................................................................... 1
2. References ............................................................................................................... 2
3. Definitions, symbols and abbreviations ................................................................. 2
   3.1 Definitions ........................................................................................................ 3
   3.2 Symbols .......................................................................................................... 3
   3.3 Abbreviations ............................................................................................... 3
4. Procedures and Signaling Flows ........................................................................... 5
   4.1 PCRF Procedures .......................................................................................... 5
   4.1.1 Initial Receipt of Service Information ....................................................... 5
   4.1.2 AGW initiated requests .......................................................................... 5
   4.1.3 Gate function ............................................................................................ 6
   4.1.4 Session modification .............................................................................. 6
   4.1.5 Loss of flow notification ......................................................................... 6
   4.1.6 AF Session Termination ......................................................................... 6
   4.1.7 Indication of IP flow release .................................................................. 6
   4.1.8 Notification of Signaling Path Status ..................................................... 6
   4.2 AF Procedures .............................................................................................. 7
   4.2.1 Provision of Service Information at session establishment .................. 7
   4.2.2 Flow Establishment ................................................................................ 7
   4.2.3 Gate function ........................................................................................... 8
   4.2.4 Session modification .............................................................................. 8
   4.2.5 Flow Release .......................................................................................... 8
   4.2.6 Subscription to Notification of Signaling Path Status ............................ 8
   4.2.7 Session Termination .............................................................................. 8
   4.3 IMS related P-CSCF procedures .................................................................. 9
   4.3.1 Provision of service information by P-CSCF ......................................... 9
   4.3.2 Enabling of IP Flows at P-CSCF .............................................................. 9
   4.4 AF Service Information association to IP-CAN Flows ............................... 10
   4.5 AF session establishment or modification .................................................. 10
   4.6 Request of Policy Information .................................................................... 12
   4.7 Change or Removal of Policy Information at AF initiated session release .. 14
   4.8 Flow Release .............................................................................................. 16
5. Tx Protocol ........................................................................................................ 18
   5.1 Protocol Support .......................................................................................... 18
   5.2 Securing Diameter messages ....................................................................... 18
   5.3 Tx messages ................................................................................................. 18
   5.3.1 A-A-Request (AAR) command ............................................................... 19
   5.3.2 A-A-Answer (AAA) command ............................................................... 19
   5.3.3 Re-Auth-Request (RAR) command ....................................................... 19
   5.3.4 Re-Auth-Answer (RAA) command ........................................................ 20
   5.3.5 Session-Termination-Request (STR) command ..................................... 20
   5.3.6 Session-Termination-Answer (STA) command ...................................... 21
   5.3.7 Abort-Session-Request (ASR) command .............................................. 21
   5.3.8 Abort-Session-Answer (ASA) command ............................................. 21
   5.4 Experimental Result/ Experimental-Result-Code AVP values .................. 22
   5.4.1 Experimental-Result AVP Message Format .......................................... 22
   5.4.2 Experimental-Result-Code AVP ............................................................. 22
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.5</td>
<td>Tx interface specific AVPs</td>
</tr>
<tr>
<td>5.5.1</td>
<td>Abort-Cause AVP</td>
</tr>
<tr>
<td>5.5.2</td>
<td>Access-Network-Charging-Address AVP</td>
</tr>
<tr>
<td>5.5.3</td>
<td>Access-Network-Charging-Identifier AVP</td>
</tr>
<tr>
<td>5.5.4</td>
<td>Access-Network-Charging-Identifier-Value AVP</td>
</tr>
<tr>
<td>5.5.5</td>
<td>AF-Application-Identifier AVP</td>
</tr>
<tr>
<td>5.5.6</td>
<td>AF-Charging-Identifier AVP</td>
</tr>
<tr>
<td>5.5.7</td>
<td>Codec-Data AVP</td>
</tr>
<tr>
<td>5.5.8</td>
<td>Flow-Description AVP</td>
</tr>
<tr>
<td>5.5.9</td>
<td>Flow-Number AVP</td>
</tr>
<tr>
<td>5.5.10</td>
<td>Flows AVP</td>
</tr>
<tr>
<td>5.5.11</td>
<td>Flow-Status AVP</td>
</tr>
<tr>
<td>5.5.12</td>
<td>Flow-Usage AVP</td>
</tr>
<tr>
<td>5.5.13</td>
<td>Specific-Action AVP</td>
</tr>
<tr>
<td>5.5.14</td>
<td>Max-Requested-Bandwidth-DL AVP</td>
</tr>
<tr>
<td>5.5.15</td>
<td>Max-Requested-Bandwidth-UL AVP</td>
</tr>
<tr>
<td>5.5.16</td>
<td>Media-Component-Description AVP</td>
</tr>
<tr>
<td>5.5.17</td>
<td>Media-Component-Number AVP</td>
</tr>
<tr>
<td>5.5.18</td>
<td>Media-Sub-Component AVP</td>
</tr>
<tr>
<td>5.5.19</td>
<td>Media-Type AVP</td>
</tr>
<tr>
<td>5.5.20</td>
<td>RR-Bandwidth AVP</td>
</tr>
<tr>
<td>5.5.21</td>
<td>RS-Bandwidth AVP</td>
</tr>
<tr>
<td>5.5.22</td>
<td>SIP-Forking-Indication AVP</td>
</tr>
<tr>
<td>5.5.23</td>
<td>Access-Network-Physical-Access-ID AVP</td>
</tr>
<tr>
<td>5.5.24</td>
<td>Access-Network-Physical-Access-ID-Value AVP</td>
</tr>
<tr>
<td>5.5.25</td>
<td>Access-Network-Physical-Access-ID-Realm AVP</td>
</tr>
<tr>
<td>5.6</td>
<td>Tx Re-used AVPs</td>
</tr>
<tr>
<td>6</td>
<td>Binding Mechanism</td>
</tr>
<tr>
<td>6.1</td>
<td>Overview</td>
</tr>
<tr>
<td>6.2</td>
<td>Session Binding</td>
</tr>
<tr>
<td>6.3</td>
<td>PCC Rule Authorization</td>
</tr>
<tr>
<td>6.4</td>
<td>Bearer Binding</td>
</tr>
<tr>
<td>A.1</td>
<td>QoS parameter mapping</td>
</tr>
<tr>
<td>A.1.1</td>
<td>Overview of QoS parameter mapping</td>
</tr>
<tr>
<td>A.2</td>
<td>QoS parameter mapping in the core network</td>
</tr>
<tr>
<td>A.2.1</td>
<td>SDP parameters to service information mapping in AF</td>
</tr>
<tr>
<td>A.2.2</td>
<td>Tx service information to Authorized IP QoS parameters mapping in PCRF</td>
</tr>
<tr>
<td>A.2.3</td>
<td>Authorized IP QoS parameters to Authorized access network QoS parameters mapping in AGW</td>
</tr>
<tr>
<td>A.2.4</td>
<td>Comparing against the Authorized access network QoS parameters in AGW</td>
</tr>
<tr>
<td>A.3</td>
<td>QoS parameter mapping in the UE</td>
</tr>
<tr>
<td>A.3.1</td>
<td>Framework for QoS mapping in the UE</td>
</tr>
<tr>
<td>A.3.2</td>
<td>SDP to access network QoS parameter mapping in UE</td>
</tr>
<tr>
<td>A.3.3</td>
<td>SDP parameters to Authorized access network QoS parameters mapping in UE</td>
</tr>
<tr>
<td>Appendix B (normative): Flow identifiers: Format definition and examples</td>
<td></td>
</tr>
<tr>
<td>B.1</td>
<td>Format of a flow identifier</td>
</tr>
<tr>
<td>B.2</td>
<td>Example 1</td>
</tr>
<tr>
<td>B.3</td>
<td>Example 2</td>
</tr>
<tr>
<td>Appendix C (normative): Support for SIP forking</td>
<td></td>
</tr>
<tr>
<td>C.1</td>
<td>Support for SIP forking</td>
</tr>
<tr>
<td>C.1.1</td>
<td>Authorization of resources for early media for forked responses</td>
</tr>
<tr>
<td>C.1.2</td>
<td>Updating the authorization information at the final answer</td>
</tr>
</tbody>
</table>
List of Figures

Figure 4.1: AF session establishment or modification.................................................................11
Figure 4.2: Policy Information Request..................................................................................13
Figure 4.3: Change or Removal of Policy Information at AF initiated session release............15
Figure 4.4: Bearer Release.......................................................................................................17
Figure A.1: Framework for QoS mapping between AF and AGW........................................36
Figure A.2: Framework for generating requested QoS parameters in the UE.......................46
List of Tables

Table 5.1-1: Tx specific 3GPP Diameter AVPs .................................................................24
Table 5.1-2: Tx specific 3GPP2 Diameter AVPs .................................................................25
Table A.2.1.1: Rules for derivation of service information within Media-Component-Description AVP from SDP media component .........................................................................................................................37
Table A.2.1.2: Rules for derivation of Media-Sub-Component AVP from SDP media component .................................................................39
Table A.2.2.1: Rules for derivation of the Maximum Authorized Data Rates and Maximum Authorized QoS Class per flow identifier in the PCRF ..........................................................................................41
Table A.2.2.2: Rules for calculating the Maximum Authorized Data Rates and QCI in the PCRF .................................................................44
Table A.2.3.1: Rules for derivation of the Authorized access network QoS Parameters per bearer from the Authorized IP QoS Parameters in AGW ..........................................................................................................................44
Table A.3.2.1: Recommended rules for derivation of the requested Maximum and Guaranteed Bitrate DL/UL per media component in the UE .........................................................................................................................47
Table A.3.3.1: Rules for derivation of the Maximum Authorized Bandwidth DL/UL and the Maximum Authorized Traffic Class per flow identifier in the UE .........................................................................................................................48
Table A.3.3.2: Rules for calculating the Maximum Authorized Bandwidths and Maximum Authorized Traffic Class per bearer in the UE .........................................................................................................................50
Table B.1: The values of the SDP parameters sent by the UE in example 1. .........................................................................................................................52
Table B.2: The values of the SDP parameters sent by the AF in example 1. .........................................................................................................................52
Table B.3: Flow identifiers in example 1. .........................................................................................................................53
Table B.4: The values of the SDP parameters sent by the UE in example 2. .........................................................................................................................53
Table B.5: The values of the SDP parameters sent by the AF in example 2. .........................................................................................................................54
Table B.6: Flow identifiers in example 2. .........................................................................................................................54
Foreword

(This foreword is not part of this document).

This document was prepared by 3GPP2 TSG-X.

This document is part of the series of documents X.S0013.

This document contains portions of material copied from 3GPP document number(s)TS 29.214. The copyright on the 3GPP document is owned by the Organizational Partners of 3GPP (ARIB - Association of Radio Industries and Businesses, Japan; CCSA – China Communications Standards Association, China; ETSI – European Telecommunications Standards Institute; ATIS – Alliance for Telecommunication Industry Solutions, USA; TTA - Telecommunications Technology Association, Korea; and TTC – Telecommunication Technology Committee, Japan), which have granted license for reproduction and for use by 3GPP2 and its Organizational Partners.
# Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Content Changes</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial publication.</td>
<td>December 2007</td>
</tr>
</tbody>
</table>
1 Introduction

This document addresses the Stage-3 protocol between an Application Function (AF) and a Policy and Charging Rules Function (PCRF) in support of Service Based Bearer Control as described in [1]. The reference point between the AF and the PCRF is designated as the Tx reference point.

The Tx interface shall allow interactions between the AF and the PCRF for the purpose of local authorization of bearer level QoS resources based on the resources negotiated at the application layer and/or based on local policy. In addition, it supports the passing of information that may be used to establish flow based charging policy. Features of the Tx interface include the following:

1. Provision and removal of application level service and flow control information from the AF to the PCRF;
2. Request of application level service and flow control information from the PCRF to the AF;
3. Notification of bearer level events from the PCRF to the AF; and
4. Application control of the flow of packets on the bearer including the restriction of flow end-points (flow filtering).
2 References

2.1 Normative 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, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] 3GPP2 X.S0013-012: “Service Based Bearer Control – Stage 2”.
[4] Void
[10] Void
[12] 3GPP2 X.S0013-004-A: "IP multimedia call control protocol based on SIP and SDP; stage 3".

2.1 Informative References

[C.S0046] 3GPP2 C.S0046: "3G Multimedia Streaming Services".
[C.S0055] 3GPP2 C.S0055: "Packet Switched Video Telephony Services (PSVT/MCS)".
3 Definitions, symbols and abbreviations

3.1 Definitions

Application Function: The Application Function (AF) is the element that requests the application of restrictions on the use of bearer resources. The Application Function represents the application level intelligence for any service running over the IP bearer, which uses Service Based Bearer Control.

NOTE: One example of an AF is the P-CSCF of the IM-CN subsystem.

AF Session: A subscriber service application level session established by an application level signaling 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.

IP Flow Establishment: An IP Flow may be established either through a reservation process such as RSVP or by the exchange of packets with a new IP address/port.

Loss of Flow: Loss of flow is used to indicate that the IP-CAN resources associated with an IP flow are released. How this is detected by the IP-CAN is IP-CAN specific.

User Transport Subscription ID: The user transport subscription ID is the user identity used to access the IP-CAN.

Service Information: The set of information conveyed from the AF to the PCRF over the Tx interface to be used as a basis for PCC decisions at the PCRF, including information about the AF session (e.g. application identifier, type of media, bandwidth, IP address and port number).

For the purpose of this document, the following terms and definitions given in [1] apply:

IP Flow
Packet Flow
Service Data Flow

3.2 Symbols

For the purposes of the present document the following symbols apply:

Tx The reference point between an AF and a PCRF

Ty The reference point between a PCRF and an AGW

3.3 Abbreviations

For the purposes of the present document the following abbreviations apply.

AAA AA-Answer
AAR AA-Request
AF Application Function
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGW</td>
<td>Access Gateway</td>
</tr>
<tr>
<td>ASA</td>
<td>Abort-Session-Answer</td>
</tr>
<tr>
<td>ASR</td>
<td>Abort-Session-Request</td>
</tr>
<tr>
<td>AVP</td>
<td>Attribute-Value Pair</td>
</tr>
<tr>
<td>IANA</td>
<td>Internet Assigned Numbers Authority</td>
</tr>
<tr>
<td>ID</td>
<td>Identifier</td>
</tr>
<tr>
<td>IMS</td>
<td>IP Multimedia Subsystem</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IP-CAN</td>
<td>IP Connectivity Access Network</td>
</tr>
<tr>
<td>MMD</td>
<td>Multimedia Domain</td>
</tr>
<tr>
<td>NASREQ</td>
<td>Network Access Server Application</td>
</tr>
<tr>
<td>PCRF</td>
<td>Policy and Charging Rules Function</td>
</tr>
<tr>
<td>P-CSCF</td>
<td>Proxy - Call Session Control Function</td>
</tr>
<tr>
<td>RAA</td>
<td>Re-Auth-Answer</td>
</tr>
<tr>
<td>RAR</td>
<td>Re-Auth-Request</td>
</tr>
<tr>
<td>SBBC</td>
<td>Service Based Bearer Control</td>
</tr>
<tr>
<td>SDI</td>
<td>Session Description Information</td>
</tr>
<tr>
<td>SIP</td>
<td>Session Initiation Protocol</td>
</tr>
<tr>
<td>STA</td>
<td>Session-Termination-Answer</td>
</tr>
<tr>
<td>STR</td>
<td>Session-Termination-Request</td>
</tr>
</tbody>
</table>
4 Procedures and Signaling Flows

4.1 PCRF Procedures

4.1.1 Initial Receipt of Service Information

The AF provides initial service information to the PCRF in the AA-Request. An AF may communicate with multiple PCRFs. The AF shall contact the appropriate H-PCRF based on the Subscription-Id AVP associated with this application session (e.g., IMS Private ID). The Subscription-Id AVP must resolve to the same H-PCRF as the user transport subscription ID. If the AA-Request contains the Media-Component-Description AVP(s) the PCRF shall store the values for the session based on the service information. If the Specific Action AVP is present in the AAR command, the PCRF shall store the requested notifications for the related IP flows.

The PCRF shall check whether the received Service Information requires PCC Rules to be provided to the AGW. This may depend on the service information and on whether the PCRF has previously been contacted by an AGW for this user.

If the PCRF identifies that PCC Rules need to be provisioned, the PCRF shall immediately send a Diameter RA-Request to the AGW to install new PCC Rules as required based on the Service Information.

The PCRF shall send an AA-Answer back to the AF. If the PCRF needs to terminate the Tx session before it has sent the AA-Answer, the PCRF shall send the AA-Answer immediately and before the AS-Request.

4.1.2 AGW initiated requests

When receiving an authorization request from the Ty interface, the PCRF shall authorize the request according to the stored policy for the session, if available. If the PCRF is acting as a V-PCRF [1], the request is routed on to a H-PCRF based on the Destination-Realm, Destination-Host, and Subscription-Id associated with the request.

If service information is not available for the session where an associated AF has been identified, or if the PCRF has already authorized the same IP flows and not obtained updated service information since then, or if the AF has instructed the PCRF to do so, the PCRF 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 PCRF shall determine whether or not to authorize the required QoS resources and shall store the service information for the session.

After the IP flow authorization, the PCRF shall send possible new access network charging identifier(s), received from the AGW during the IP flow authorization, to the AF for charging correlation purposes, and an access network charging-address, if the AF has instructed the PCRF to do so. The PCRF does this by sending the Re-Auth-Request message with the CHARGING_CORRELATION_EXCHANGE indication in the Specific-Action AVP to the AF.

If the PCRF receives a notification that an IP flow(s) is being established via the Ty interface and the PCRF associates IP flow(s) described in the Service Information of an AF session with the IP flow(s) identified, and if the corresponding AF has requested a notification of IP flow establishment from the PCRF, the PCRF shall send a RA-Request including the Specific Action AVP with the value set to INDICATION_OF_ESTABLISHMENT_OF_FLOW and shall indicate the affected IP flows with the Flows AVP(s).
4.1.3  Gate function

Depending on the application, in the Service Information provision, the AF may instruct the PCRF as part of the Media-Component-Description AVP(s) whether the media IP flow(s) should be enabled or disabled at the IP flow authorization. The PCRF may receive a separate AA-Request message(s) from the AF to enable or disable specified IP flows. Based on this, the PCRF may decide to install or remove the corresponding Charging Rule(s).

If a Media-Sub-Component AVP under a Media-Component-Description AVP contains a Flow-Usage AVP with the value RTCP, then the corresponding RTCP IP Flows in both directions shall be enabled even if the Flow-Status AVP under the Media-Sub-Component AVP is set to ENABLED-UPLINK, ENABLED-DOWNLINK, ENABLED, or DISABLED.

The PCRF shall reply with an AA-Answer and shall include the Access-Network-Charging-Identifier(s) available at this moment. The PCRF makes the final decision to enable or disable the authorized IP flows.

4.1.4  Session modification

The PCRF may receive the AA-Request message from the AF with modified service information. The PCRF shall process the received updated Service Information in Media-Component-Description AVP(s) according to the operator policy and may decide whether the request is accepted or not. If accepted, the PCRF shall update the Service Information with the new information received. Due to the updated Service Information, the PCRF may need to create, modify or delete the related PCC rules and authorized QoS and provide the updated information towards the AGW following the corresponding procedures specified at Ty.

The PCRF 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 been supplied earlier to the AF.

4.1.5  Loss of flow notification

If the AF has requested a notification at the loss of a flow, and the PCRF receives a notification over the Ty interface that a flow is lost, the PCRF shall send a Re-Auth-Request with the value for the Specific-Action AVP set to INDICATION_OF_LOSS_OF_FLOW and shall indicate the affected IP flows with the Flows AVP(s).

4.1.6  AF Session Termination

When an AF session is terminated, the AF shall send a Session-Termination-Request command to the PCRF.

The PCRF shall send a Session-Termination-Answer to the AF.

4.1.7  Indication of IP flow release

If the PCRF receives a CC-Request from the AGW with an indication of IP flow termination, the PCRF shall check for each of the IP flows from AF Service Information, if it needs to notify the corresponding AF (i.e., if the AF has requested a notification at the release of an IP flow). The PCRF shall send a Diameter RA-Request in order to notify the AF. Within the RA-Request, the PCRF shall set the value for the Specific-Action AVP to INDICATION_OF_TERMINATION_OF_FLOW, shall indicate the affected IP flows with the Flows AVP(s) and shall provide the appropriate Abort-Cause AVP value.

4.1.8  Notification of Signaling Path Status

In the event that the PCRF is notified of the Loss of Resources associated to the PCC Rules corresponding with AF Signalling IP Flows, the PCRF shall inform the AF about the Loss of the Signalling Transmission path by sending a
Re-Authorization Request (RAR) command to the AF. The RAR shall include the Specific-Action AVP set to the value "INDICATION_OF_LOSS_OF_FLOW".

When the AF receives the RAR command, it shall acknowledge the command by sending an RAA command to the PCRF.

The AF may then decide to terminate the Tx Diameter session used for the notification of the status of the AF Signalling transmission path. The AF may also decide to terminate any other active Tx Diameter session with the PCRF related to the AF Signalling which is not available any longer. In that case, the AF shall then initiate the AF Termination procedure towards the PCRF as defined in clause 4.2.7.

4.2 AF Procedures

4.2.1 Provision of Service Information at session establishment

When a new AF session is being established and media information for this AF session is available at the AF, the AF shall open an Tx Diameter session with the PCRF using a AA-Request command. The AF shall provide the UE's IP address which is used by the UE for communicating with the AF using either Framed-IP-Address AVP or Framed-IPv6-Prefix AVP, and the corresponding Service Information within Media-Component-Description AVP(s). The AF shall indicate to the PCRF as part of the Media-Component-Description whether the media IP flow(s) should be enabled or disabled with the Flow-Status AVP.

An AF may communicate with multiple PCRFs. The AF shall contact the appropriate H-PCRF based on the Subscription-Id AVP associated with this application session (e.g., IMS Private ID). The Subscription-ID provided by the AF must resolve to the same H-PCRF as the user transport subscription ID. The AF may also include the AF-Charging-Identifier AVP into the message for the charging correlation purposes. The AF may also include the Specific-Action AVP to request notification for certain events, e.g., IP flow termination or IP flow establishment.

To allow the PCRF to match the described service IP flows in an unambiguous manner with TFT filter information, the AF shall supply both source and destination IP addresses and port numbers within the Flow-Description AVP, if such information is available.

The AF may request notifications of specific IP-CAN Session events through the usage of the Specific Action AVP in the AA-Request command. The PCRF shall make sure to inform the AF of the requested notifications in the event that they take place.

The behavior when the AF does not receive the AA-Answer, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different than DIAMETER_SUCCESS, are outside the scope of this specification and based on operator policy.

4.2.2 Flow Establishment

The PCRF 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 PCRF when receiving a Re-Auth-Request message with a request for the service information.

The AF may receive an access network charging identifier and access network charging address for charging correlation purposes from the PCRF in a separate Re-Auth-Request message after the flow 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 and access network charging address.
4.2.3 Gate function

The AF shall indicate to the PCRF as part of the Media-Component-Description whether the media IP flow(s) should be enabled or disabled at the flow authorization. Depending on the application, in the Service Information provision, the AF may instruct the PCRF 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.

If a Media-Sub-Component AVP under a Media-Component-Description AVP contains a Flow-Usage AVP with the value RTCP, then the corresponding RTCP IP Flows in both directions shall be enabled even if the Flow-Status AVP under the Media-Sub-Component AVP is set to ENABLED-UPLINK, ENABLED-DOWNLINK, ENABLED, or DISABLED.

The behavior when the AF does not receive the AAA, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different than DIAMETER_SUCCESS, are outside the scope of this specification and based on operator policy.

4.2.4 Session modification

During the AF session modification, the AF shall send AA-Request command to the PCRF containing the Media-Component-Description AVP(s) with the updated Service Information.

The behavior when the AF does not receive the AAA, or when it arrives after the internal timer waiting for it has expired, or when it arrives with an indication different than DIAMETER_SUCCESS, are outside the scope of this specification and based on operator policy.

4.2.5 Flow Release

When AF session is terminated the AF shall revoke the corresponding IP flow(s) authorization by the sending Session-Termination-Request message to the PCRF.

Upon the reception of a Re-Auth-Request including an Abort-Cause AVP indicating that some of the IP flows (included in the Flows AVP) of the AF session are being discontinued, the AF will issue a Re-Auth-Answer as a response to the PCRF.

4.2.6 Subscription to Notification of Signaling Path Status

An AF may subscribe to notifications of the status of the IP flow associated with AF Signaling. To do so, the AF shall open an Tx Diameter session with the PCRF using an AA-Request command. The AF shall provide the UE's IP address which is used by the UE for communicating with the AF (using either the Framed-IP-Address AVP or the Framed-IPv6-Prefix AVP) and the Specific-Action AVP requesting the subscription to "INDICATION_OF_LOSS_OF_FLOW". The AF shall additionally provide a Media-Component-Description AVP including a single Media-Sub-Component AVP with the Flow-Usage AVP set to the value "AF_SIGNALLING".

The AF may cancel the subscription to notifications of the IP flow associated with the status of the AF Signalling at any time. In that case, the AF shall use a Session-Termination-Request (STR) command to the PCRF, which shall be acknowledged with a Session-Termination-Answer (STA) command.

4.2.7 Session Termination

When an AF session is terminated, the AF shall send Session-Termination-Request command to the PCRF.

When the PCRF receives a ST-Request from the AF, indicating an AF session termination, it shall free the resources allocated for the corresponding Service Data Flow(s). The PCRF shall initiate the request for the removal of any related PCC rules from the AGW and for the update of the Authorized QoS for the affected IP flows.

The PCRF shall send a ST-Answer to the AF.
4.3 IMS related P-CSCF procedures

4.3.1 Provision of service information by P-CSCF

The P-CSCF shall send service information to the PCRF upon receipt of a 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 PCRF receives proper information to perform media authorization for all possible IMS session set-up scenarios, and that the PCRF 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 service information from every SDP media component. The SDP contains sufficient information about the session, such as the end-points’ IP addresses 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 P-CSCF of UE B uses the address present in this SDP for the destination address of UE B's uplink Flow-Description AVP, while the P-CSCF 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.

- A 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 P-CSCF of UE B uses the address present in this SDP for the destination address of UE A's downlink Flow-Description AVP, while the P-CSCF 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. For the possibly associated RTCP IP flows, the P-CSCF shall use the SDP "b=RR" and "b=RS" parameters, if present. 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, and RTP payload, or IP, UDP and RTCP.

4.3.2 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 or 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. 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. 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, e.g., after the 200 OK(INVITE) is received, the P-CSCF shall provide the Flow-Status AVPs as derived from the SDP.
4.4  **AF Service Information association to IP-CAN Flows**

Binding refers to the PCRF process of associating IP flows described in AF service information with policy information associated with the related user and service.

If an IP flow described in the AF service information is subject to separate charging, the PCRF shall install a Charging Rule with a Service Data Flow Filter matching this IP flow.

NOTE: The PCRF process of deriving PCC Rules from AF service information depends on operator preferences and is not fully specified.

Upon the release of an IP flow or other bearer events, the PCRF notifies AF(s) about the IP flow release.

The following methods for binding are available:

- UE identity information (e.g. NAI, IMSI or MSISDN) is used for binding purposes.

- It is also recommended to use TFT filters (from AGW via Ty) and Flow-Description AVPs provided within the service information (from AF via Tx) to select the Charging Rules matching to an IP flow.

- Also the QoS information (negotiated QoS from the AGW and QoS information derived from the service information provided by the AF) may be used for further analysis.

A charging rule does not necessarily identify a single bearer for an IP flow described in AF Service Information, therefore the same Charging Rule may be installed over several bearers, even if it corresponds only to a single AF session IP flow.

4.5  **AF session establishment or modification**

This clause covers the provision of service information and related QoS authorization and/or PCC Rules when an AF session is being established or modified.
1. The AF receives an internal or external trigger to provide Service Information, at a set-up of a new AF session or at a modification of an existing AF session.

2. The AF identifies the Service Information needed (e.g. IP address of the IP flow(s), port numbers to be used etc…).

3. The AF provides the Service Information to the PCRF by sending a Diameter AAR for a new Tx Diameter session at set-up of a new AF session, or for the existing Tx Diameter session in case of AF session modification.

4. The PCRF shall store the received Service Information

5. The PCRF identifies any affected IP flows described in the AF Service Information.
If any affected IP flow(s) are identified in step 5, steps 6 through 14 are performed. If there are no IP flow(s) affected, steps 6 through 14 are not executed.

6. The PCRF sends Diameter RAR to trigger the AGW to request policy information.

7. The AGW sends RAA to acknowledge the RAR.

8. The Policy Information is requested by the AGW, using the Diameter CCR. The AGW also provides information about the IP flows within the request.

9. The PCRF stores the received IP flow information in the Diameter CCR, e.g. TFT filters and UE IP address (prefix).

10. The PCRF binds the IP flows to all matching IP flow(s) of existing of AF session(s) using the IP flows information received from the AGW and the Service Information received from the AF(s).

11. The PCRF defines new Policy Information to be installed for the identified IP flows (e.g., new charging rule or authorized QoS). For a modified IP flow, the PCRF can also identify existing Policy Information that needs to be modified or removed. The Policy Information may relate to any of the matching AF sessions identified in step 10 or that may exist in the PCRF without matching to any AF session.

12. The PCRF stores the selected Policy Information for the IP flows.

13. The Policy Information is provisioned by the PCRF to the AGW using Diameter CCA. The PCRF may also provide event triggers listing IP flow events for which the PCRF desires Policy Information Requests.

14. The AGW installs the received Policy Information. For a modified IP flow the AGW may also have to modify or remove previously installed Policy Information.

15. The PCRF sends a Diameter AAA to the AF. This may be done anytime following step 3.

### 4.6 Request of Policy Information

This clause covers both the PCRF-initiated and bearer-event-initiated Request of Policy Information by the AGW. Policy information may include QoS authorization, charging rules, gating information, etc.

A bearer-event-initiated Request of Policy Information occurs when a new bearer is established or when an existing bearer is modified. For the Packet Data Subsystem, these are Service Instance Activation(s) or Modification(s). A bearer modification event triggers a Policy Information request from the AGW to the PCRF only if the PCRF has previously installed an event-trigger at the AGW for the given bearer modification event.

A PCRF-initiated Request of Policy Information is achieved by a Diameter RAR sent from the PCRF. The RAR request may occur in several scenarios, as depicted in Figures 4.1 – 4.4. An AGW-initiated Request of PCC Rules may also happen as a consequence of a bearer-event-initiated Request of PCC Rules, as shown in figure 4.2.
Figure 4.2: Policy Information Request.

1. The AGW receives a trigger for a Policy Information Request, such as the establishment or modification of an IP flow or an RAR from the PCRF.

2. The Policy Information is requested by the AGW, using the Diameter CCR. The AGW also provides information about the IP flow within the request.

3. The PCRF stores the received IP flow information in the Diameter CCR, e.g. TFT filters and UE IP address (prefix).

4. The PCRF associates the IP flow to all matching IP flow(s) of existing of AF session(s) using the IP flow information received from the AGW and the Service Information received from the AF(s).

5. The PCRF defines new Policy Information to be installed for the identified IP flow (e.g., new charging rule or authorized QoS). For a modified IP flow, the PCRF can also identify existing Policy Information that needs to be modified or removed. The Policy Information may relate to any of the matching AF sessions identified in step 4 or that may exist in the PCRF without matching to any AF session.

6. The PCRF stores the selected Policy Information for the IP flow.
7. The Policy Information is provisioned by the PCRF to the AGW using Diameter CCA. The PCRF may also provide event triggers listing IP flow events for which the PCRF desires Policy Information Requests.

8. The AGW installs the received Policy Information. For a modified IP flow the AGW may also have to modify or remove previously installed Policy Information.

If the trigger in step 1 was a IP flow establishment, steps 9 and 10 are executed separately for each affected AF session for which the AF has requested notification of IP flow establishment.

9. The PCRF sends a Diameter RAR to the AF to inform it about the IP flow establishment.

10. The PCRF sends RAA to acknowledge the RAR.

### 4.7 Change or Removal of Policy Information at AF initiated session release

This clause covers the change or removal of Policy Information at the AF session release.
1. The AF receives an internal or external trigger for a session release.

2. The AF sends a session termination request, Diameter STR, to the PCRF to request the removal of the session.

Figure 4.3: Change or Removal of Policy Information at AF initiated session release
3. The PCRF identifies where Policy Information for the IP flow(s) of this AF session are installed. This Policy Information needs to be changed or removed.

If any affected IP flow(s) are identified in step 3, steps 4 through 12 are performed. If there are no IP flow(s) affected, steps 4 through 12 are not executed.

4. The PCRF sends a Diameter RAR to trigger the AGW to request Policy Information.

5. The AGW sends a Diameter RAA to acknowledge the RAR.

6. The Policy Information is requested by the AGW, using the Diameter CCR. The AGW also provides information about the IP flows within the request.

7. The PCRF stores the received IP flow information in the Diameter CCR, e.g. TFT filters and UE IP address (prefix).

8. The PCRF binds the IP flows to all matching IP flow(s) of existing of AF session(s) using the IP flows information received from the AGW and the Service Information received from the AF(s).

9. The PCRF defines new Policy Information to be installed for the identified IP flows (e.g., new charging rule or authorized QoS). For a modified IP flow, the PCRF can also identify existing Policy Information that needs to be modified or removed. The Policy Information may relate to any of the matching AF sessions identified in step 10 or that may exist in the PCRF without matching to any AF session.

10. The PCRF stores the selected Policy Information for the IP flows.

11. The Policy Information is provisioned by the PCRF to the AGW using Diameter CCA. The PCRF may also provide event triggers listing IP flow events for which the PCRF desires Policy Information Requests.

12. The AGW installs the received Policy Information. For a modified IP flow the AGW may also have to modify or remove previously installed Policy Information.

13. The PCRF sends a Diameter STA to the AF. This may be done anytime following step 2.

### 4.8 Flow Release

This clause covers the release of one or more flows, which may be indicated to the AF. Two cases are covered:

- bearer release that does not cause IP flow(s) within an AF session to be disabled;
- bearer release that causes some or all of the IP flow(s) within an AF session to be disabled.

Bearer release may not cause an IP flow within an AF session to be disabled. For the Packet Data Subsystem, the PCRF does not necessary know which Service Instance carries the IP flow, thus a release of a Service Instance does not necessarily mean that the IP flow is disabled. For flows associated with a specific Service Instance, the flow identifiers need to be provided to the PCRF.
1. A bearer is deactivated. For the Packet Data Subsystem, the PDSN deactivates the Service Instance carrying IP flow(s).

2. The AGW sends a Diameter CCR message to the PCRF, indicating the set of flows that are terminated.

3. The PCRF marks the Policy Information for the terminated flows as changed or removed.

4. The PCRF acknowledges the flow termination by sending a Diameter CCA message.

The following steps apply for each AF where at least one IP Flow within an AF session is being disabled. The steps shall be performed separately for each ongoing AF session that is affected by the bearer release as explained below.

5. The PCRF indicates the release of the flows by sending a Diameter RAR to the AF.

6. The AF responds by sending a Diameter RAA to the PCRF.

7. The AF may send an AAR to the PCRF to update the session information.

8. If step 7 occurs, the PCRF responds by sending a AAA to the AF.
5     Tx Protocol

5.1     Protocol Support

The Diameter Base Protocol as specified in [2] shall apply except as modified by the defined procedures and AVPs in the present document. Unless otherwise specified, the procedures (including error handling and unrecognized information handling) are unmodified.

In addition to the AVPs defined within the clause 5.5, the Diameter AVPs from the Diameter base application [2] are reused within the Diameter messages sent over the Tx interface. The support of AVPs from the Diameter Network Access Server Application (NASREQ) [3] 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 Tx interface.

The present document re-uses the Diameter application defined for the 3GPP Rx interface. The Rx Diameter application is defined as an IETF vendor specific Diameter application with application ID 16777236, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

Due to the definition of the commands used in Tx protocol, there is no possibility to skip the Auth-Application-Id AVP and use the Vendor-Specific-Application-Id AVP instead. Therefore the Tx application identifier shall be included in the Auth-Application-Id AVP.

With regard to the Diameter protocol defined over the Tx interface, the PCRF acts as a Diameter server, in the sense that it is the network element that handles QoS authorization requests and charging rules for a particular realm. The AF acts as the Diameter Client, in the sense that is the network element requesting QoS authorization to use bearer path network resources or charging control with respect to these resources.

The AF and the PCRF shall advertise the support of the Rx specific Application by including the value 16777236 of the application identifier in the Auth-Application-Id AVP and the value of the 3GPP (10415) in the Vendor-Id AVP within the Vendor Specific-Application-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. The AF and PCRF shall advertise support of 3GPP2 and 3GPP vendor-specific AVPs by including the vendor identifier value of 3GPP2 (5535) within a Supported-Vendor-Id AVP, and the vendor identifier value of 3GPP (10415) within a Supported-Vendor-Id AVP of the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in the Diameter Base Protocol.

5.2     Securing Diameter messages

For secure transport of Diameter messages, see [2].

5.3     Tx messages

Existing Diameter command codes from the Diameter base protocol [2] and the NASREQ Diameter application [3] are used with the Tx specific AVPs. A Tx specific Auth-Application id is used together with the command code to identify the Tx 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.
NOTE: Some of the AVPs included in the messages formats below are in bold to highlight that these AVPs are used by this specific protocol and do not belong to the original Diameter Base Protocol [2] or NASREQ Diameter application [3].

5.3.1 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 PCRF 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-State-Id ]
  { Origin-Realm } [ Destination-Host ]
  { Destination-Realm } [ Proxy-Info ]
  [ Media-Component-Description ] [ SIP-Forking-Indication ] [ AVP ]
  [ AF-Charging-Identifier ]
  [ Specific-Action ] [ Failed-AVP ]
  [ Subscription-ID ]
  [ Experimental-Result ]
  [ Access-Network-Charging-Identifier ] [ Access-Network-Charging-Address ] [ Access-Network-Physical-Access-ID ]
  [ Origin-State-Id ] [ Proxy-Info ] [ AVP ]
```

5.3.2 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 PCRF to the AF in response to the AAR command.

Message Format:

```
<AA-Answer> ::= < Diameter Header: 265, PXY >
  < Session-Id >
  { Auth-Application-Id } [ Access-Network-Charging-Identifier ]
  { Origin-Host } [ Access-Network-Charging-Address ] [ Access-Network-Physical-Access-ID ]
  { Origin-State-Id } [ Proxy-Info ] [ AVP ]
  [ Result-Code ] [ Experimental-Result ] [ Failed-AVP ]
  [ Error-Message ] [ Error-Reporting-Host ] [ Redirect-Host ]
  [ Redirect-State-Id ] [ Redirect-State-Usage ] [ Redirect-Max-Cache-Time ] [ Failed-AVP ]
  [ Proxy-Info ] [ AVP ]
```

5.3.3 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 PCRF to the AF in order to indicate a specific action.
As an option, the AF may send an AAR command to the PCRF to update the service information when receiving an RAR command. However, application-specific authentication and/or authorization messages are not mandated for the Tx interface in response to an RAR command.

The values INDICATION_OF_LOSS_OF_FLOW, INDICATION_OF_RECOVERY_OF_FLOW and INDICATION_OF_RELEASE_OF_FLOW of the 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 }
  { Specific-Action }
  *[ Access-Network-Charging-Identifier ]
  [ Access-Network-Charging-Address ]
  *[ Flows ]
  *[ Subscription-ID ]
  [ Abort-Cause ]
  [ Origin-State-Id ]
  *[ Class ]
  *[ Proxy-Info ]
  *[ Route-Record ]
  *[ AVP ]

5.3.4 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 PCRF in response to the RAR command.

Message Format:

<RA-Answer> ::= < Diameter Header: 258, PXY >
  < Session-Id >
  { Origin-Host }
  { Origin-Realm }
  [ Result-Code ]
  [ Experimental-Result ]
  *[ Media-Component-Description ]
  [ Origin-State-Id ]
  *[ Class ]
  [ Error-Message ]
  [ Error-Reporting-Host ]
  *[ Redirect-Host ]
  [ Redirect-Host-Usage ]
  [ Redirect-Max-Cache-Time ]
  *[ Failed-AVP ]
  *[ Proxy-Info ]
  *[ AVP ]

5.3.5 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 PCRF that an authorized session shall be terminated.

Message Format:

<ST-Request> ::= < Diameter Header: 275, REQ, PXY >
  < Session-Id >
  { Origin-Host }
  { Origin-Realm }
5.3.6  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 PCRF to the AF in response to the STR command.

Message Format:

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

5.3.7  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 PCRF to inform the AF that all bearer resources for the authorized session have become unavailable. The Abort-Cause AVP although not defined in [2], is required and is specific to the Tx interface (See 5.5.1).

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 ]
   *[ Class ]
   *[ Proxy-Info ]
   *[ Route-Record ]
   *[ AVP ]

5.3.8  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 PCRF in response to the ASR command.

Message Format:

<AS-Answer> ::= < Diameter Header: 274, PXY >
   < Session-Id >
   { Origin-Host }
5.4 Experimental Result/ Experimental-Result-Code AVP values

5.4.1 Experimental-Result AVP Message Format

The Experimental-Result AVP (AVP Code 297) which is defined in [2] is of type Grouped, and indicates whether a particular vendor-specific request was completed successfully or whether an error occurred.

Message Format:

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

The Vendor-Id AVP identifies the vendor responsible for the assignment of the experimental result code which follows. All Diameter answer messages defined in vendor-specific applications shall include either one Result-Code AVP or one Experimental-Result AVP. Unless otherwise indicated, Vendor-Id AVP shall have the value of 10415 (3GPP) for Experimental-Result-Code specified in this document.

5.4.2 Experimental-Result-Code AVP

The Experimental-Result-Code AVP (AVP Code 298) is of type Unsigned32 and contains a vendor-assigned value representing the result of processing the request.

Specific values of the Experimental-Result-Code AVP for Tx interface use:

INVALID_SERVICE_INFORMATION (5061)

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

FILTER_RESTRICTIONS (5062)

The Flow_Description AVP(s) cannot be handled by the PCRF because restrictions defined in clause 5.5.8 are not observed.

REQUESTED_SERVICE_NOT_AUTHORIZED (5063)

The requested service, as described by the service information provided by the AF, is not consistent with either the related subscription information or operator defined policy rules.

DUPlicated_AF_SESSION (5064)

The PCRF rejects a new Tx session setup because the new Tx session relates to an AF session with another related active Tx session, e.g. if the AF provided the same AF charging identifier for this new Tx session that is already in use for the other ongoing Tx session.
5.5  **Tx interface specific AVPs**

Table 5.1-1 describes the 3GPP Diameter AVPs not included in the Diameter base protocol [2] and used for the Tx 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 3GPP Diameter AVPs defined in the present document shall be set to 10415 (3GPP).

Table 5.1-2 describes the 3GPP2 Diameter AVPs not included in the Diameter base protocol [2] and used for the Tx 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 3GPP2 Diameter AVPs defined in the present document shall be set to 5535 (3GPP2).
Table 5.1-1: Tx specific 3GPP Diameter AVPs

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Clause defined</th>
<th>Value Type (note 2)</th>
<th>Must</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May Encr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abort-Cause</td>
<td>500</td>
<td>5.5.1</td>
<td>Enumerated</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Access-Network-Charging-Address</td>
<td>501</td>
<td>5.5.2</td>
<td>Address</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Access-Network-Charging-Identifier</td>
<td>502</td>
<td>5.5.3</td>
<td>Grouped</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Access-Network-Charging-Identifier-Value</td>
<td>503</td>
<td>5.5.4</td>
<td>OctetString</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>AF-Application-Identifier</td>
<td>504</td>
<td>5.5.5</td>
<td>OctetString</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>AF-Charging-Identifier</td>
<td>505</td>
<td>5.5.6</td>
<td>OctetString</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Codec-Data</td>
<td>524</td>
<td>5.5.7</td>
<td>OctetString</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Flow-Description</td>
<td>507</td>
<td>5.5.8</td>
<td>IPFilterRule</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Flow-Number</td>
<td>509</td>
<td>5.5.10</td>
<td>Unsigned32</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Flows</td>
<td>510</td>
<td>5.5.11</td>
<td>Grouped</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Flow-Status</td>
<td>511</td>
<td>5.5.12</td>
<td>Enumerated</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Flow-Usage</td>
<td>512</td>
<td>5.5.13</td>
<td>Enumerated</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Specific-Action</td>
<td>513</td>
<td>5.5.14</td>
<td>Enumerated</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Max-Requested-Bandwidth-DL</td>
<td>515</td>
<td>5.5.16</td>
<td>Unsigned32</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Max-Requested-Bandwidth-UL</td>
<td>516</td>
<td>5.5.17</td>
<td>Unsigned32</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Media-Component-Description</td>
<td>517</td>
<td>5.5.18</td>
<td>Grouped</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Media-Component-Number</td>
<td>518</td>
<td>5.5.19</td>
<td>Unsigned32</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Media-Sub-Component AVP</td>
<td>519</td>
<td>5.5.20</td>
<td>Grouped</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>Media-Type</td>
<td>520</td>
<td>5.5.21</td>
<td>Enumerated</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>RR-Bandwidth</td>
<td>521</td>
<td>5.5.22</td>
<td>Unsigned32</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>RS-Bandwidth</td>
<td>522</td>
<td>5.5.23</td>
<td>Unsigned32</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
<tr>
<td>SIP-Forking-Indication</td>
<td>523</td>
<td>5.5.24</td>
<td>Enumerated</td>
<td>M,V</td>
<td>P</td>
<td></td>
<td></td>
<td>Y</td>
</tr>
</tbody>
</table>

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 [2].

NOTE 2: The value types are defined in [2].
Table 5.1-2: Tx specific 3GPP2 Diameter AVPs

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>AVP Code</th>
<th>Clause defined</th>
<th>Value Type (note 2)</th>
<th>Must</th>
<th>May</th>
<th>Should not</th>
<th>Must not</th>
<th>May Encr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access-Network-Physical-ID</td>
<td>900</td>
<td>5.5.23</td>
<td>Grouped</td>
<td>V</td>
<td>P</td>
<td>M</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Access-Network-Physical-ID-Value</td>
<td>899</td>
<td>5.5.24</td>
<td>OctetString</td>
<td>V</td>
<td>P</td>
<td>M</td>
<td>Y</td>
<td></td>
</tr>
<tr>
<td>Access-Network-Physical-ID-Realm</td>
<td>898</td>
<td>5.5.25</td>
<td>OctetString</td>
<td>V</td>
<td>P</td>
<td>M</td>
<td>Y</td>
<td></td>
</tr>
</tbody>
</table>

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 [2].

NOTE 2: The value types are defined in [2].

5.5.1 Abort-Cause AVP

The 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 flow release. The following values are defined:

FLOW_RELEASED (0)

This value is used when the flow has been deactivated as a result from normal signalling handling.

INSUFFICIENT_SERVER_RESOURCES (1)

This value is used to indicate that the PCRF 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. PDSN for PDS).

5.5.2 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 PDSN IP address). The Access-Network-Charging-Address AVP should not be forwarded over an inter-operator interface.

5.5.3 Access-Network-Charging-Identifier AVP

The Access-Network-Charging-Identifier AVP (AVP code 502) is of type Grouped, and contains a charging identifier 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 PCRF to the AF. The AF may use this information for charging correlation with session layer.

AVP Format:

```plaintext
Access-Network-Charging-Identifier ::= < AVP Header: 502 >
    { Access-Network-Charging-Identifier-Value }
    *[ Flows ]
```
5.5.4 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.

5.5.5 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 PCRF 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 Ty interface is selected. The AF-Application-Identifier may be used also to complete the QoS authorization with application specific default settings in the PCRF if the AF does not provide full Session-Component-Description information.

5.5.6 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.

5.5.7 Codec-Data AVP

The Codec-Data AVP (AVP code 524) is of type OctetString.

The Codec-Data AVP shall contain codec related information known at the AF. This information shall be encoded as follows:

- The first line shall be the direction of the SDP used to derive the information, i.e. "uplink" or "downlink".

  NOTE: The majority of the information within the Codec-Data AVP indicating "downlink" describes properties of the sender of the SDP, for instance receiver capabilities, and is therefore applicable for IP flows in the uplink direction. Similarly, the majority of the information within the Codec-Data AVP indicating "uplink" describes properties of the sender of the SDP, for instance receiver capabilities, and is therefore applicable for IP flows in downlink direction.

- The second line of the value of the Codec-Data AVP shall consist of either the word "offer" or the word "answer", or the word "description" (in ASCII, without quotes) followed by a new-line character. The semantics of these words are the following:

  - "offer" indicates that SDP lines from an SDP offer according to [9] are being provisioned in the Codec-Data AVP.

  - "answer" indicates that SDP lines from an SDP answer according to [9] are being provisioned in the Codec-Data AVP.

  - "description" indicates that SDP lines from a SDP session description in a scenario where the offer-answer mechanism of [9] is not being applied are being provisioned in the Codec-Data AVP. For instance, SDP from an RTSP "Describe" reply may be provisioned.

- The rest of the value shall consist of SDP line(s) in ASCII encoding separated by new-line characters, as specified in [8]. The first of these line(s) shall be an "m" line. The remaining lines shall 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 do not need to be included.

5.5.8 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 (the Source Port may be omitted to indicate that any source port is allowed; for the Tx interface, lists or ranges shall not be used).

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 PCRF 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.

5.5.9 **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 A.

5.5.10 **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 ]
```

5.5.11 **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.

5.5.12 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.

AF_SIGNALING (2)

This value is used to indicate that the IP flow is used to transport AF Signalling Protocols (e.g. SIP/SDP).

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 the PCRF.

5.5.13 Specific-Action AVP

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

Within a Re-Authorization Request, the 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 PCRF 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 an 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 PCRF requests the service information from the AF for the bearer event. In the AAR, this value indicates that the AF requests the PCRF to demand service information at each bearer authorization.

CHARGING_CORRELATION_EXCHANGE (1)

Within a RAR, this value shall be used when the PCRF 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 PCRF to provide an access network charging identifier to the AF at each bearer establishment/modification, when a new access network charging identifier becomes available.

INDICATION_OF_LOSS_OF_FLOW (2)

Within a RAR, this value shall be used when the PCRF reports a loss of a bearer to the AF. In the AAR, this value indicates that the AF requests the PCRF to provide a notification at the loss of a flow.
INDICATION_OF_RECOVERY_OF_FLOW (3)

Within a RAR, this value shall be used when the PCRF reports a recovery of a flow to the AF. In the AAR, this value indicates that the AF requests the PCRF to provide a notification at the recovery of a flow.

INDICATION_OF_RELEASE_OF_FLOW (4)

Within a RAR, this value shall be used when the PCRF reports the release of a flow to the AF. In the AAR, this value indicates that the AF requests the PCRF to provide a notification at the release of a flow.

INDICATION_OF_ESTABLISHMENT_OF_FLOW (5)

Within a RAR, this value shall be used when the PCRF reports the establishment of a flow to the AF. In the AAR, this value indicates that the AF requests the PCRF to provide a notification at the establishment of a flow.

5.5.14 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.

5.5.15 Max-Requested-Bandwidth-UL AVP

The Max-Requested-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.

5.5.16 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 PCRF 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 PCRF may delete corresponding filters and state information.

Each Media-Component-Description AVP shall contain either zero, or one, or two Codec-Data AVPs. In the case of conflicts, information contained in other AVPs either within this Media-Component-Description AVP, or within the corresponding Media-Component-Description AVP in a previous message, shall take precedence over information within the Codec-Data AVP(s). The AF shall provision all the available information in other applicable AVPs in addition to the information in the Codec-Data AVP, if such other AVPs are specified.

If the SDP offer-answer procedures of [9] are applicable for the session negotiation between the two ends taking part in the communication (e.g., for IMS), the following applies:

- The AF shall provision information derived from an SDP answer and shall also provision information derived from the corresponding SDP offer.
If the Media-Component-Description AVP contains two Codec-Data AVPs, one of them shall represent an SDP offer and the other one the corresponding SDP answer.

- If the Media-Component-Description AVP contains one Codec-Data AVP, and this AVP represents an SDP offer, the AF shall provision the corresponding SDP answer information in a Codec-Data AVP within a subsequent Tx message.

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 packetisation time within the "a=ptime" line. Other parameters within the SDP answer take precedence over corresponding parameters within the SDP offer.

If SDP is applied without using the offer-answer procedures, zero or one Codec-Data AVP shall be provisioned:

AVP format:

Media-Component-Description ::= < AVP Header: 517>
{ 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 ]
[*[ Codec-Data ]

5.5.17 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 A.

5.5.18 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 Annex A.

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 PCRF may delete corresponding filters and state information.

AVP format:

Media-Sub-Component ::= < AVP Header: 519>
{ 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 ]
### 5.5.19 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)
- TEXT (5)
- MESSAGE (6)
- OTHER (0xFFFFFFFF)

### 5.5.20 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 [6]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP.

### 5.5.21 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 [6]. The bandwidth contains all the overhead coming from the IP-layer and the layers above, i.e. IP, UDP and RTCP.

### 5.5.22 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.

### 5.5.23 Access-Network-Physical-Access-ID AVP

The Access-Network-Physical-Access-ID AVP (AVP code 900) is of type Grouped. It is used to convey, for charging purposes, a value and realm that identifies the access network topology segment that is serving the UE. The 3GPP2 vendor ID 5535 shall be used for this AVP.

**AVP Format:**

```plaintext
Access-Network-Physical-Access-ID ::= < AVP Header: 900 >
{ Access-Network-Physical-Access-ID-Value }
{ Access-Network-Physical-Access-ID-Realm }
*[ AVP ]
```
### 5.5.24 Access-Network-Physical-Access-ID-Value AVP

The Access-Network-Physical-Access-ID-Value AVP (AVP code 899) is of type OctetString and it conveys an identifier used to denote a topological segment of the access network that is serving the UE. The semantics of the Access-Network-Physical-Access-ID-Value AVP is specific to the access network type (RAT-Type AVP) and Access-Network-Physical-Access-ID-Realm AVP. The 3GPP2 vendor ID 5535 shall be used for this AVP.

### 5.5.25 Access-Network-Physical-Access-ID-Realm AVP

The Access-Network-Physical-Access-ID-Realm AVP (AVP code 898) is of type OctetString and it conveys the administrative realm in which the Access-Network-Physical-Access-ID-Value AVP refers to. This realm may differ from the Origin-Realm AVP in the Diameter request, and allows the PCRF to properly disambiguate different access network physical access identifier values within and across different Diameter signaling realms, access technology types, and/or PLMNs. The 3GPP2 vendor ID 5535 shall be used for this AVP.

### 5.6 Tx Re-used AVPs

The table 5.6.1 lists the Diameter AVPs re-used by the Rx reference point from existing Diameter Applications, including a reference to their respective specifications and when needed, a short description of their usage within the Tx reference point. Other AVPs from existing Diameter Applications, except for the AVPs from Diameter Base Protocol, do not need to be supported. The AVPs from Diameter Base Protocol are not included in table 5.6.1, but they are re-used for the Tx protocol.

<table>
<thead>
<tr>
<th>Attribute Name</th>
<th>Reference</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscription-Id</td>
<td>[7]</td>
<td>The identification of the subscription (IMSI, MSISDN, etc.)</td>
</tr>
<tr>
<td>Framed-IP-Address</td>
<td>[3]</td>
<td>The valid routable IPv4 address that is applicable for the IP Flows towards the UE at the PCEF. The PCRF shall use this address to identify the correct IP-CAN session (session binding).</td>
</tr>
<tr>
<td>Framed-IPv6-Prefix</td>
<td>[3]</td>
<td>The valid routable IPv6 address prefix that is applicable for the IP Flows towards the UE at the PCEF. The PCRF shall use this address to identify the correct IP-CAN session (session binding).</td>
</tr>
</tbody>
</table>
6 Binding Mechanism

6.1 Overview

The binding mechanism associates the session information provided by the AF with the IP-CAN bearer that is intended to carry the service data flow.

The binding mechanism includes three steps:

- Session binding.
- PCC Rule authorization.
- Bearer binding.

The Session Binding function receives the Session Information and determines the relevant IP-CAN session. With this information the PCC Rule Authorization function runs the policy rules and constructs the PCC rule(s) if the authorization is granted. Finally the Bearer Binding function selects the IP-CAN bearer where the PCC rule(s) should be installed within the IP-CAN session already known.

PCC Rule Authorization and Bearer Binding can take place without Session Binding at certain IP-CAN Session events (e.g. IP-CAN Session Establishment).

6.2 Session Binding

Session binding is the association of the AF session information and applicable PCC rules to an IP-CAN session.

When the PCRF accepts an AA-Request from the AF over the Tx interface with service information, the PCRF shall perform session binding and associate the described service IP flows within the AF session information (and therefore the applicable PCC rules) to an existing IP-CAN session. This association is done using the user IP address received via the Tx interface in either the Framed-IP-Address AVP, or the Framed-IPv6-Prefix AVP. The Subscription-Id AVP, the Flow-Description AVP, or both may also assist in this association. A given Tx Session may be bound to one or more Ty sessions. Typically such multiple bindings occur when an UE uses different IP addresses for different media streams (audio, video etc) in a session or if the UE uses different IP addresses for signaling and media.

The PCRF will determine that the UE has an IP-CAN session if the UE has established a connection path to the PDS where the AF is connected to.

As a result from the session binding function, the PCRF identifies what IP-CAN session the current AF session is related with. If the PCRF is not capable of executing the Session Binding, the PCRF shall issue an AA-Answer command to the AF with a negative response.

6.3 PCC Rule Authorization

The PCRF shall perform the PCC rule authorization when it receives session information from an AF over Tx interface or when it receives notification of IP-CAN session events (e.g. establishment, modification) from the AGW over Ty interface. The PCRF shall also perform PCC Rule Authorization for dynamic PCC Rules already provisioned to the AGW due to internal PCRF triggers (e.g. policies are included or modified within PCRF). The PCRF assigns an appropriate QCI to each PCC rule.

When PCC Rule Authorization is executed after successful Session Binding, the PCRF shall authorize the affected PCC rules. By this process the PCRF will determine whether the user can have access to the requested services and under what constraints. If so, the PCC rules are created or modified. If the Session Information is not authorized, a negative answer shall be issued to the AF by sending an AA-Answer command.
The PCRF assigns an appropriate QCI to each PCC rule. IP-CAN specific restrictions and other information available to the PCRF (e.g. users subscription information, operator policies) shall be taken into account. Each PCC rule shall receive a QoS class QCI that can be supported by the IP-CAN.

6.4 Bearer Binding

The Bearer Binding function is responsible for associating a PCC rule to an IP-CAN bearer within the IP-CAN session. The AGW is responsible for implementing this function. The QoS demand in the PCC rule and the service data flow template are input to the bearer binding. The selected bearer shall have the same QCI as the one indicated by the PCC rule.

NOTE: For an IP-CAN, limited to a single IP-CAN bearer per IP-CAN session, the bearer is implicit, so finding the IP-CAN session is sufficient for successful bearer binding.

The PCRF shall supply the PCC rules to be installed, modified or removed over Ty interface to the AGW. The AGW shall then check the QCI indicated by the PCC Rule(s) and bind the PCC rule with an IP-CAN bearer that has the same QCI.
Annex A (normative):

A.1 QoS parameter mapping

A.1.1 Overview of QoS parameter mapping

The AF derives information about the service from the session description information or from other sources. The AF passes service information to the PCRF. The PCRF notes and authorizes the IP flows described within this service information by mapping from service information to Authorized IP QoS parameters for transfer to the AGW via the Ty interface. The AGW will map from the Authorized IP QoS parameters to the Authorized access network QoS parameters.

The UE derives the authorized access network QoS parameters in an application specific manner. It should use information from the AF session signalling and session description information for that purpose. If SDP is used as session description information, the UE may apply the mapping rules within this document.

Upon receiving the bearer activation or modification, the AGW shall compare the access network QoS parameters against the authorized access network QoS parameters. If the request lies within the limits authorized by the PCRF, the bearer activation or modification shall be accepted.

Figure A.1 indicates the network entities where QoS mapping functionality is performed. This mapping is performed by:

1. If SBBC is applied then the AF may map from session description information within the AF session signalling to service information passed to the PCRF over the Tx interface. The mapping is application specific. If SDP is used as session description information, the AF should apply the mapping described in Clause A.2.1. For IMS, the mapping rules in Clause A.2.1 shall be used at the P-CSCF.

2. The PCRF shall map from the service information received over the Tx interface to the Authorized IP QoS parameters that shall be passed to the AGW via the Ty interface. The mapping is performed for each flow identifier.

3. The UE derives access network QoS parameters from the AF session signalling in an application specific manner for each flow identifier. The access network QoS parameters should be generated according to application demands and recommendations for conversational or streaming applications. If SDP is used as session description information, e.g. for IMS, the UE may apply Clause A.3.2. In case the UE multiplexes several IP flows onto the same bearer, it has to combine their IP and access network QoS parameters.

4. The AGW shall map from the Authorized IP QoS parameters received from PCRF to the Authorized access network QoS parameters (see Clause A.2.3).

5. The AGW shall compare the access network QoS parameters of the bearer against the Authorized access network QoS parameters (see Clause A.2.4).

The mapping that takes place in the UE and the network should be compatible in order to ensure that the AGW will be able to correctly authorize the session.
### A.2 QoS parameter mapping in the core network

#### A.2.1 SDP parameters to service information mapping in AF

Within IMS, session establishment and modification involves an end-to-end message-exchange using SIP/SDP with negotiation of media attributes (e.g. Codecs) as defined in [12]. If the IMS applies Service Based bearer Control then the P-CSCF shall provide service information derived from the relevant SDP information to the PCRF via the Tx interface. The P-CSCF shall apply the mapping rules in Table A.2.1.1 to derive service information from SDP. The SIP/SDP message will also have been passed on to the UE, where the UE will perform its own mapping from the SDP parameters and application demands to some access network QoS parameters in order to populate the requested QoS field within the bearer activation or modification.

The mapping described in this clause is mandatory for the P-CSCF and should also be applied by other AFs if the session description information is SDP.

When a session is initiated or modified the P-CSCF shall use the mapping rules in Table A.2.1.1 for each SDP media component to derive a Media-Component-Description AVP from the SDP Parameters.
Table A.2.1.1: Rules for derivation of service information within Media-Component-Description AVP from SDP media component

<table>
<thead>
<tr>
<th>service information per Media-Component-Description AVP (NOTE 1; NOTE 7)</th>
<th>Derivation from SDP Parameters (see NOTE 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media-Component-Number</td>
<td>ordinal number of the position of the &quot;m=&quot; line in the SDP</td>
</tr>
<tr>
<td>AF-Application-Identifier</td>
<td>The AF-Application-Identifier AVP may be supplied or omitted, depending on the application. For IMS, if the AF-Application-Identifier AVP is supplied, its value should not demand application specific bandwidth or QoS class handling. However, if an IMS application is capable of handling a QoS downgrading, the AF-Application-Identifier AVP may be used to demand application specific bandwidth or QoS class handling.</td>
</tr>
<tr>
<td>Media-Type</td>
<td>The Media Type AVP shall be included with the same value as supplied for the media type in the &quot;m=&quot; line.</td>
</tr>
<tr>
<td>Flow-Status</td>
<td>IF port in m-line = 0 THEN Flow-Status:= REMOVED; ELSE IF a=recvonly THEN IF &lt;SDP direction&gt; = mobile originated THEN Flow-Status := ENABLED_DOWNLINK; (NOTE 4) ELSE /* mobile terminated <em>/ Flow-Status := ENABLED_UPLINK; (NOTE 4) ENDIF; ELSE IF a=sendonly THEN IF &lt;SDP direction&gt; = mobile originated THEN Flow-Status := ENABLED_UPLINK; (NOTE 4) ELSE /</em> mobile terminated <em>/ Flow-Status := ENABLED_DOWNLINK; (NOTE 4) ENDIF; ELSE IF a=inactive THEN Flow-Status :=DISABLED; ELSE /</em> a=sendrecv or no direction attribute */ Flow-Status := ENABLED; (NOTE 4) ENDIF; ENDIF; ENDIF; ENDIF; (NOTE 5)</td>
</tr>
<tr>
<td>Max-Requested-Bandwidth-UL</td>
<td>IF &lt;SDP direction&gt; = mobile terminated THEN IF b=AS:&lt;bandwidth&gt; is present THEN Max-Requested-Bandwidth-UL:= &lt;bandwidth&gt; * 1000; /* Unit is bit/s ELSE Max-Requested-Bandwidth-UL:= &lt;Operator specific setting&gt;, or AVP not supplied; ENDIF; ELSE Consider SDP in opposite direction ENDIF</td>
</tr>
<tr>
<td>Max-Requested-Bandwidth-DL</td>
<td>IF &lt;SDP direction&gt; = mobile originated THEN IF b=AS:&lt;bandwidth&gt; is present THEN Max-Requested-Bandwidth-DL:= &lt;bandwidth&gt; * 1000; /* Unit is bit/s ELSE Max-Requested-Bandwidth-DL:= &lt;Operator specific setting&gt;, or AVP not supplied; ENDIF; ELSE Consider SDP in opposite direction ENDIF</td>
</tr>
<tr>
<td>RR-Bandwidth</td>
<td>IF b=RR:&lt;bandwidth&gt; is present THEN RR-Bandwidth:= &lt;bandwidth&gt;; ELSE</td>
</tr>
</tbody>
</table>

37
<table>
<thead>
<tr>
<th>Media-Sub-Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supply one AVP for each Flow Identifier within the media component. The Flow identifiers are derived according to Appendix A. The encoding of the AVP is described in Table A.2.1.2</td>
</tr>
</tbody>
</table>

**NOTE 1:** The encoding of the service information is defined in [1].

**NOTE 2:** The SDP parameters are described in [8].

**NOTE 3:** The 'b=RS:' and 'b=RR:' SDP bandwidth modifiers are defined in [6].

**NOTE 4:** As an operator policy to disable forward and/or backward early media, the Flow-Status may be downgraded before a SIP dialogue is established, i.e. until a 200 OK(INVITE) is received. The Value "DISABLED" may be used instead of the Values "ENABLED_UPLINK" or "ENABLED_DOWNLINK". The Values "DISABLED", "ENABLED_UPLINK" or "ENABLED_DOWNLINK" may be used instead of the Value "ENABLED".

**NOTE 5:** If the SDP answer is available when the session information is derived, the direction attributes and port number from the SDP answer shall be used to derive the flow status. However, to enable interoperability with SIP clients that do not understand the inactive SDP attribute, if a=inactive was supplied in the SDP offer, this shall be used to derive the flow status. If the SDP answer is not available when the session information is derived, the direction attributes from the SDP offer shall be used.

**NOTE 6:** Information from the SDP answer is applicable, if available.

**NOTE 7:** The AVPs may be omitted if they have been supplied in previous service information and have not changed, as detailed in [1].
Table A.2.1.2: Rules for derivation of Media-Sub-Component AVP from SDP media component

<table>
<thead>
<tr>
<th>Tx service information per Media-Sub-Component AVP (NOTE 1, NOTE 5)</th>
<th>Derivation from SDP Parameters (see NOTE 2)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flow-Number</strong></td>
<td>derived according to Appendix B</td>
</tr>
<tr>
<td>The AF shall assign a number to the media-subcomponent AVP that is unique within the surrounding media component AVP and for the entire lifetime of the AF session. The AF shall select the ordinal number of the IP flow(s) within the &quot;m=&quot; line assigned in the order of increasing downlink destination port numbers, if downlink destination port numbers are available. For uplink or inactive unicast media IP flows, a downlink destination port number is nevertheless available, if SDP offer-answer according to [9] is used. The AF shall select the ordinal number of the IP flow(s) within the &quot;m=&quot; line assigned in the order of increasing uplink destination port numbers, if no downlink destination port numbers are available.</td>
<td></td>
</tr>
<tr>
<td><strong>Flow-Status</strong></td>
<td>AVP not supplied</td>
</tr>
<tr>
<td><strong>Max-Requested-Bandwidth-UL</strong></td>
<td>AVP not supplied</td>
</tr>
<tr>
<td><strong>Max-Requested-Bandwidth-DL</strong></td>
<td>AVP not supplied</td>
</tr>
<tr>
<td><strong>Flow-Description</strong></td>
<td>For uplink and dowlink direction, a Flow-Description AVP shall be provided unless no IP flows in this direction are described within the media component. The SDP direction attribute (NOTE 4) indicates the direction of the media IP flows within the media component as follows:</td>
</tr>
<tr>
<td>IF a=recvonly THEN (NOTE 3)</td>
<td>IF &lt;SDP direction&gt; = mobile originated THEN</td>
</tr>
<tr>
<td>ELSE /* mobile terminated */</td>
<td>Provide only downlink Flow-Description AVP</td>
</tr>
<tr>
<td>ENDIF;</td>
<td>ENDIF;</td>
</tr>
<tr>
<td>ELSE</td>
<td>IF a=sendonly THEN (NOTE 3)</td>
</tr>
<tr>
<td>IF &lt;SDP direction&gt; = mobile originated THEN</td>
<td>IF &lt;SDP direction&gt; = mobile originated THEN</td>
</tr>
<tr>
<td>ELSE /* mobile terminated */</td>
<td>Provide only downlink Flow-Description AVP</td>
</tr>
<tr>
<td>ENDIF;</td>
<td>ENDIF;</td>
</tr>
<tr>
<td>ELSE /* a=sendrecv or a=inactive or no direction attribute */</td>
<td>Provide uplink and downlink Flow-Description AVPs</td>
</tr>
<tr>
<td>ENDIF;</td>
<td>ENDIF;</td>
</tr>
<tr>
<td>For RTCP IP flows uplink and downlink Flow-Description AVPs shall be provided irrespective of the SDP direction attribute. The uplink destination address shall be copied from the &quot;c=&quot; line of downlink SDP. (NOTE 6) The uplink destination port shall be derived from the &quot;m=&quot; line of downlink SDP. (NOTE 6) The downlink destination address shall be copied from the &quot;c=&quot; line of uplink SDP. (NOTE 6) The downlink destination port shall be derived from the &quot;m=&quot; line of uplink SDP. (NOTE 6) Uplink and downlink source addresses shall either be derived from the prefix of the destination address or be wildcarded by setting to &quot;any&quot;, as specified in [1]. Source ports shall not be supplied. Proto shall be derived from the transport of the &quot;m=&quot; line. For &quot;RTP/AVP&quot; proto is 17(UDP).</td>
<td></td>
</tr>
<tr>
<td><strong>Flow-Usage</strong></td>
<td>The Flow-Usage AVP shall be supplied with value &quot;RTCP&quot; if the IP flow(s) described in the Media-Sub-Component AVP are used to transport RTCP. Otherwise the Flow-Usage AVP shall not be supplied. [8] specifies how RTCP flows are described within SDP.</td>
</tr>
</tbody>
</table>
### A.2.2 Tx service information to Authorized IP QoS parameters mapping in PCRF

The QoS authorization process consists of the derivation of the parameters Authorized QoS Class Identifier (QCI) and Authorized Maximum/Guaranteed Data Rate UL/DL.

When a session is initiated or modified the PCRF shall use the mapping rules in Table A.2.2.1 to derive the Authorized IP QoS parameters (i.e., QCI, Authorized Maximum/Guaranteed Data Rate DL/UL) from the service information. In the case of forking, the various forked responses may have different QoS requirements for the IP flows of the same media component. Each Authorized IP QoS Parameter shall be set to the highest value requested for the IP flow(s) of that media component by any of the active forked responses. These values are derived by the rules in Table A.2.2.1.
Table A.2.2.1: Rules for derivation of the Maximum Authorized Data Rates and Maximum Authorized QoS Class per flow identifier in the PCRF

<table>
<thead>
<tr>
<th>Authorized IP QoS Parameter per flow identifier</th>
<th>Derivation from service information (see NOTE 4)</th>
</tr>
</thead>
</table>
| Maximum Authorized Data Rate DL (Max_DR_DL) and UL (Max_DR_UL) per flow identifier | IF operator special policy exists THEN  
    Max_DR_UL := as defined by operator specific algorithm;  
    Max_DR_DL := as defined by operator specific algorithm;  
ELSE   
    IF AF-Application-Identifier AVP demands application specific data rate handling THEN  
        Max_DR_UL := as defined by application specific algorithm;  
        Max_DR_DL := as defined by application specific algorithm;  
    ELSE   
        IF Codec-Data AVP provides Codec information for a codec that is supported by a specific algorithm THEN  
            (NOTE 5)  
            Max_DR_UL := as defined by the specific algorithm;  
            Max_DR_DL := as defined by the specific algorithm;  
        ELSE   
            IF not RTCP flow(s) according to Flow-Usage AVP THEN  
                IF Flow-Status = REMOVED THEN  
                    Max_DR_UL := 0;  
                    Max_DR_DL := 0;  
                ELSE  
                    IF uplink Flow Description AVP is supplied THEN  
                        IF Max-Requested-Bandwidth-UL is present THEN  
                            Max_DR_UL := Max-Requested-Bandwidth-UL;  
                        ELSE  
                            Max_DR_UL := as set by the operator;  
                        ENDIF  
                    ELSE  
                        Max_DR_UL := 0;  
                    ENDIF;  
                ENDIF;  
            ENDIF;  
            IF downlink Flow Description AVPs is supplied THEN  
                IF Max-Requested-Bandwidth-DL is present THEN  
                    Max_DR_DL := Max-Requested-Bandwidth-DL;  
                ELSE  
                    Max_DR_DL := as set by the operator;  
                ENDIF  
            ELSE  
                Max_DR_DL := 0;  
            ENDIF;  
        ELSE  
            Max_DR_DL := as set by the operator;  
        ENDIF;  
    ENDIF;  
ELSE /* RTCP IP flow(s) */  
    IF RS-Bandwidth is present and RR-Bandwidth is present THEN  
        Max_DR_UL := (RS-Bandwidth + RR-Bandwidth);  
        Max_DR_DL := (RS-Bandwidth + RR-Bandwidth);  
    ELSE  
        IF Max-Requested-Bandwidth-UL is present THEN  
            IF RS-Bandwidth is present and RR-Bandwidth is not present THEN  
                Max_DR_UL := MAX(0.05 * Max-Requested-Bandwidth-UL, RS-Bandwidth);  
            ENDIF;  
            IF RS-Bandwidth is not present and RR-Bandwidth is present THEN  
                Max_DR_UL := MAX(0.05 * Max-Requested-Bandwidth_UL, RR-Bandwidth);  
            ENDIF;  
            IF RS-Bandwidth and RR-Bandwidth is not present THEN  
                Max_DR_UL := 0.05 * Max-Requested-Bandwidth_UL;  
            ENDIF;  
        ELSE  
            Max_DR_UL := as set by the operator;  
        ENDIF;  
    ENDIF;  
|
IF Max-Requested-Bandwidth-DL is present THEN
  IF RS-Bandwidth is present and
    RR-Bandwidth is not present THEN
      Max_DR_DL:= \text{MAX}[0.05 \times \text{Max-Requested-Bandwidth-DL},
      RS-Bandwidth];
    ENDIF;
  ELSE
    Max_DR_DL:= \text{as set by the operator};
  ENDIF;
  ENDIF; /* RTCP flow */
ENDIF; /* operator policy */

Authorized Guaranteed Data Rate DL (Gua_DR_DL) and
UL (Gua_DR_UL)

IF operator special policy exists THEN
  Gua_DR_UL:= \text{as defined by operator specific algorithm};
  Gua_DR_DL:= \text{as defined by operator specific algorithm};
ELSE
  IF AF-Application-Identifier AVP demands application specific data rate
  handling THEN
    Gua_DR_UL:= \text{as defined by application specific algorithm};
    Gua_DR_DL:= \text{as defined by application specific algorithm};
  ELSE
    IF Codec-Data AVP provides Codec information for a codec that is
    supported by a specific algorithm (NOTE 5) THEN
      Gua_DR_UL:= \text{as defined by specific algorithm};
      Gua_DR_DL:= \text{as defined by specific algorithm};
    ELSE
      Gua_DR_UL:= \text{Max DR UL};
      Gua_DR_DL:= \text{Max DR DL};
    ENDIF;
  ENDIF
ENDIF

ENDIF
Authorized QoS Class Identifier [QCI] per flow identifier
(see NOTES 1, 2, 3 and 7)

IF a special policy exists THEN
  QCI:= as defined by operator specific algorithm;
ELSE
  IF AF-Application-Identifier AVP demands application specific QoS Class handling THEN
    QCI:= as defined by application specific algorithm;
  ELSE
    IF Codec-Data AVP provides Codec information for a codec that is supported by a specific algorithm THEN
      QCI:= as defined by specific algorithm; (NOTE 5)
    ELSE
      IF Media-Type is present THEN
        IF only uplink Flow Description AVPs are supplied for all IP flows of the AF session, which have media type "audio" or "video" and no flow usage "RTCP", or only downlink Flow Description AVPs are supplied for all IP flows of the AF session, which have media type "audio" or "video" and no flow usage "RTCP") THEN
          MaxClassDerivation:=3 or 4; (Note 6) /*streaming*/
        ELSE
          MaxClassDerivation:=1 or 2; (Note 6) /*conversational*/
        ENDIF;
        CASE Media-Type OF
          "audio":        QCI:= MaxClassDerivation
          "video":        QCI:= MaxClassDerivation
          "application": QCI:=1 or 2; (Note 6) /*conversational*/
          "data":         QCI:=6 or 7 or 8; (Note 6) /*interactive with priority 3, 2, or 2 and SI=0*/
          "control":      QCI:=5; /*interactive with priority 1*/
          /*new media type*/
          OTHERWISE:      QCI:=9; /*background*/
        END;
      ENDIF;
    END;
  ENDIF;
ENDIF;

NOTE 1: The Maximum Authorized QoS Class for a RTCP IP flow is the same as for the corresponding RTP media IP flow.

NOTE 2: When audio or video IP flow(s) are removed from a session, the parameter MaxClassDerivation shall keep the originally assigned value.

NOTE 3: When audio or video IP flow(s) are added to a session, the PCRF shall derive the parameter MaxClassDerivation taking into account the already existing media IP flow(s) within the session.

NOTE 4: The encoding of the service information is defined in [1]. If AVPs are omitted within a Media-Component-Description AVP or Media-Sub-Component AVP of the service information, the corresponding information from previous service information shall be used, as specified in [1].

NOTE 5: 3GPP2 specifications [C.S0046] and [C.S0055] contain examples of QoS parameters for codecs of interest. The support of any codec specific algorithm in the PCRF is optional.

NOTE 6: The final QCI value will depend on the value of SSID (speech/unknown). It is recommended that the value unknown is taken to ease backwards compatibility.

NOTE 7: The numeric value of the QCI are based on QoS-Class-Identifier defined in Ty [X.S0013-013].

The PCRF shall per ongoing session store the Authorized IP QoS parameters per flow identifier.

If the PCRF provides an Authorized-QoS AVP within a Charging-Rule-Definition AVP it may apply the rules in Table A.2.2.2 to combine the Authorized QoS per IP flow or bidirectional combination of IP flows (as derived according to table A.2.2.1) for all IP flows described by the corresponding PCC rule.

If the PCRF provides an Authorized-QoS AVP for an entire IP CAN bearer or IP CAN session, it may apply the rules in table A.2.2.2 to combine the Authorized QoS per IP flow or bidirectional combination of IP flows (as derived according to table A.2.2.1) for all IP flows allowed to be transported within the IP CAN bearer or session. It is recommended that the rules in table A.2.2.2 are applied for all IP flows with corresponding AF session. The PCRF may increase the authorized QoS further to take into account the requirements of predefined PCC rules without ongoing AF sessions.
Table A.2.2.2: Rules for calculating the Maximum Authorized Data Rates and QCI in the PCRF

<table>
<thead>
<tr>
<th>Authorized IP QoS Parameter</th>
<th>Calculation Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Authorized Data Rate DL and UL</td>
<td>Maximum Authorized Data Rate DL/UL is the sum of all Maximum Authorized Data Rate DL/UL for all the flow identifiers.</td>
</tr>
<tr>
<td>QCI</td>
<td>QCI = MAX [needed QoS parameters per flow identifier among all the flow identifiers].</td>
</tr>
</tbody>
</table>

A.2.3 Authorized IP QoS parameters to Authorized access network QoS parameters mapping in AGW

The Translation/Mapping function in the AGW shall derive the Authorized access network QoS parameters from the Authorized IP QoS parameters received from the PCRF according to the rules in Table A.2.3.1.

Table A.2.3.1: Rules for derivation of the Authorized access network QoS Parameters per bearer from the Authorized IP QoS Parameters in AGW

<table>
<thead>
<tr>
<th>Authorized access network QoS Parameter per bearer</th>
<th>Derivation from Authorized IP QoS Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Authorized Bandwidth DL/UL per bearer</td>
<td>Maximum Authorized Bandwidth DL/UL per bearer = Maximum Authorized Data Rate DL/UL</td>
</tr>
<tr>
<td>Maximum Authorized Traffic Class per bearer</td>
<td>The mapping is based on QoS-Class-Identifier definition given in Ty [X.S0013-014].</td>
</tr>
</tbody>
</table>

A.2.4 Comparing against the Authorized access network QoS parameters in AGW

Upon receiving a bearer activation request the AGW compares the requested access network QoS parameters against the corresponding Authorized access network QoS parameters received via the translation/mapping function. If all the requested parameters lie within the limits, the bearer activation or bearer modification request shall be accepted i.e. the following criteria shall be fulfilled:

- the requested Guaranteed Bitrate DL/UL (if the requested Traffic Class is Conversational or Streaming) or Maximum Bitrate DL/UL (if the requested Traffic Class is Interactive or Background) is less than or equal to Maximum Authorized data rate DL/UL; and
- the requested Traffic Class is less than or equal to Maximum Authorized Traffic Class.

If any of the requested parameters are greater than the corresponding Authorized access network QoS parameters, the AGW shall downgrade the requested access network QoS parameters to fall within authorized values.
A.3 **QoS parameter mapping in the UE**

If the UE uses a different QoS mapping mechanism then Section A.3 does not apply.

### A.3.1 Framework for QoS mapping in the UE

Figure A.2 indicates the entities participating in the generation of the requested QoS parameters to activate or modify a bearer in the UE. The steps are:

1. The Application provides the access network QoS Manager, possibly via the Translation/Mapping function, with relevant information to perform step 2 or step 4. (Not subject to standardization).

2. If needed, information from step 1 is used to access a proper set of access network QoS Parameters (see [13]).

3. If SDP is available then the SDP Parameters should give guidance for the access network BS Manager (possibly via the Translation/Mapping function), according to the rules in clause A.3.2, to set the Maximum Bitrate UL/DL and the Guaranteed Bitrate UL/DL. Furthermore if the SDP Parameters are received in an IMS context in which SBBC is applied, the Maximum Authorized Bandwidth UL/DL and Maximum Authorised Traffic Class should be derived according to the rules in clause A.3.3.

4. A set of access network QoS Parameters values from step 2 (or directly from step 1) is possibly merged together with the Maximum Bitrate UL/DL and the Guaranteed Bitrate UL/DL from step 3. The result should constitute the requested access network QoS Parameters. If the bearer is activated or modified in an IMS context in which SBBC is applied, the UE should check that the requested Guaranteed Bitrate UL/DL or requested Maximum Bitrate UL/DL (depending on the requested Traffic Class) does not exceed the Maximum Authorized Bandwidth UL/DL derived in step 3. Furthermore, if the UE has implemented the mapping rule for Maximum Authorized Traffic Class, as defined in clause A.3.3, the UE should check that the requested Traffic Class does not exceed the Maximum Authorised Traffic Class derived in step 3.
A.3.2 SDP to access network QoS parameter mapping in UE

If SDP Parameters are available, then before activating or modifying a bearer the UE should check if the SDP Parameters give guidance for setting the requested access network QoS Parameters. The UE should use the mapping rule in table A.3.2.1 to derive the Maximum and Guaranteed Bitrate DL/UL from the SDP Parameters.
### Table A.3.2.1: Recommended rules for derivation of the requested Maximum and Guaranteed Bitrate DL/UL per media component in the UE

<table>
<thead>
<tr>
<th>access network QoS Parameter per media component</th>
<th>Derivation from SDP Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component</td>
<td>/* Check if the media use codec(s) */</td>
</tr>
<tr>
<td></td>
<td>IF [ (&lt;media&gt; = (&quot;audio&quot; or &quot;video&quot;) and &lt;transport&gt; = &quot;RTP/AVP&quot;) ] THEN</td>
</tr>
<tr>
<td></td>
<td>/* Check if Streaming */</td>
</tr>
<tr>
<td></td>
<td>IF a = (&quot;sendonly&quot; or &quot;recvonly&quot;) THEN</td>
</tr>
<tr>
<td></td>
<td>Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified in reference [5] ;</td>
</tr>
<tr>
<td></td>
<td>/* Conversational as default */</td>
</tr>
<tr>
<td></td>
<td>ELSE</td>
</tr>
<tr>
<td></td>
<td>ENDIF ;</td>
</tr>
<tr>
<td></td>
<td>/* Check for presence of bandwidth attribute for each media component */</td>
</tr>
<tr>
<td></td>
<td>ELSEIF b = AS: &lt;bandwidth-value&gt; is present THEN</td>
</tr>
<tr>
<td></td>
<td>IF media stream only downlink THEN</td>
</tr>
<tr>
<td></td>
<td>Maximum Bitrate DL = Guaranteed Bitrate DL = &lt;bandwidth-value&gt; ;</td>
</tr>
<tr>
<td></td>
<td>ELSEIF media stream only uplink THEN</td>
</tr>
<tr>
<td></td>
<td>Maximum Bitrate UL = Guaranteed Bitrate UL = &lt;bandwidth-value&gt; ;</td>
</tr>
<tr>
<td></td>
<td>ELSEIF media streams both downlink and uplink THEN</td>
</tr>
<tr>
<td></td>
<td>Maximum Bitrate DL = Guaranteed Bitrate DL = &lt;bandwidth-value&gt; ;</td>
</tr>
<tr>
<td></td>
<td>Maximum Bitrate UL = Guaranteed Bitrate UL = &lt;bandwidth-value&gt; ;</td>
</tr>
<tr>
<td></td>
<td>ENDIF ;</td>
</tr>
<tr>
<td></td>
<td>ELSE</td>
</tr>
<tr>
<td></td>
<td>/* SDP does not give any guidance ! */</td>
</tr>
<tr>
<td></td>
<td>Maximum Bitrate DL/UL and Guaranteed Bitrate DL/UL per media component as specified by the UE manufacturer ;</td>
</tr>
<tr>
<td></td>
<td>ENDIF ;</td>
</tr>
</tbody>
</table>

### A.3.3 SDP parameters to Authorized access network QoS parameters mapping in UE

If the bearer is activated or modified and SBBC is applied, then the UE should use the mapping rules in table A.3.3.1 for all applications using SDP to derive the Maximum Authorized Bandwidth UL/DL per flow identifier. Table A.3.3.1 also has a mapping rule for derivation of Maximum Authorized Traffic Class per flow identifier that applies for session initiation and modification.

In the case of forking, the various forked responses may have different QoS requirements for the same IP flows of a media component. When the Authorized access network QoS Parameters are used by the UE, they shall be set equal to the highest values requested for the IP flows of that media component by any of the active forked responses. The UE should use the mapping rule in table A.3.3.1 for each forked response.
Table A.3.3.1: Rules for derivation of the Maximum Authorized Bandwidth DL/UL and the Maximum Authorized Traffic Class per flow identifier in the UE

<table>
<thead>
<tr>
<th>Authorized access network QoS Parameter per flow identifier</th>
<th>Derivation from SDP Parameters (see NOTE 4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Authorized Bandwidth DL (Max_BW_DL) and UL (Max_BW_UL) per flow identifier (see NOTE 5)</td>
<td>IF SBBC is applied THEN</td>
</tr>
<tr>
<td></td>
<td>/* The Direction of the IP flow(s) identified by the flow identifier */</td>
</tr>
<tr>
<td></td>
<td>IF a=reconly THEN</td>
</tr>
<tr>
<td></td>
<td>IF &lt;SDP direction&gt; = mobile originated THEN</td>
</tr>
<tr>
<td></td>
<td>Direction:= downlink;</td>
</tr>
<tr>
<td></td>
<td>ELSE /* mobile terminated */</td>
</tr>
<tr>
<td></td>
<td>Direction:= uplink;</td>
</tr>
<tr>
<td></td>
<td>ENDIF;</td>
</tr>
<tr>
<td></td>
<td>ELSE;</td>
</tr>
<tr>
<td></td>
<td>IF a=sendonly THEN</td>
</tr>
<tr>
<td></td>
<td>IF &lt;SDP direction&gt; = mobile originated THEN</td>
</tr>
<tr>
<td></td>
<td>Direction:= uplink;</td>
</tr>
<tr>
<td></td>
<td>ELSE /* mobile terminated */</td>
</tr>
<tr>
<td></td>
<td>Direction:= downlink;</td>
</tr>
<tr>
<td></td>
<td>ENDIF;</td>
</tr>
<tr>
<td></td>
<td>ELSE /<em>sendrecv, inactive or no direction attribute</em>/</td>
</tr>
<tr>
<td></td>
<td>Direction:=both;</td>
</tr>
<tr>
<td></td>
<td>ENDIF;</td>
</tr>
<tr>
<td></td>
<td>ENDIF;</td>
</tr>
<tr>
<td></td>
<td>/* Max_BW_UL and Max_BW_DL */</td>
</tr>
<tr>
<td></td>
<td>IF media IP flow(s) THEN</td>
</tr>
<tr>
<td></td>
<td>IF bAS=AS:&lt;bandwidth&gt; is present THEN</td>
</tr>
<tr>
<td></td>
<td>IF Direction=downlink THEN</td>
</tr>
<tr>
<td></td>
<td>Max_BW_UL:= 0;</td>
</tr>
<tr>
<td></td>
<td>Max_BW_DL:= bAS;</td>
</tr>
<tr>
<td></td>
<td>ELSE</td>
</tr>
<tr>
<td></td>
<td>IF Direction=uplink THEN</td>
</tr>
<tr>
<td></td>
<td>Max_BW_UL:= bAS;</td>
</tr>
<tr>
<td></td>
<td>Max_BW_DL:= 0;</td>
</tr>
<tr>
<td></td>
<td>ELSE /<em>Direction=both</em>/</td>
</tr>
<tr>
<td></td>
<td>Max_BW_UL:= bAS;</td>
</tr>
<tr>
<td></td>
<td>Max_BW_DL:= bAS;</td>
</tr>
<tr>
<td></td>
<td>ENDIF;</td>
</tr>
<tr>
<td></td>
<td>ENDIF;</td>
</tr>
<tr>
<td></td>
<td>ELSE</td>
</tr>
<tr>
<td></td>
<td>bw:= as set by the UE manufacturer;</td>
</tr>
<tr>
<td></td>
<td>IF Direction=downlink THEN</td>
</tr>
<tr>
<td></td>
<td>Max_BW_UL:= 0;</td>
</tr>
<tr>
<td></td>
<td>Max_BW_DL:= bw;</td>
</tr>
<tr>
<td></td>
<td>ELSE</td>
</tr>
<tr>
<td></td>
<td>IF Direction=uplink THEN</td>
</tr>
<tr>
<td></td>
<td>Max_BW_UL:= bw;</td>
</tr>
<tr>
<td></td>
<td>Max_BW_DL:= 0;</td>
</tr>
<tr>
<td></td>
<td>ELSE /<em>Direction=both</em>/</td>
</tr>
<tr>
<td></td>
<td>Max_BW_UL:= bw;</td>
</tr>
<tr>
<td></td>
<td>Max_BW_DL:= bw;</td>
</tr>
<tr>
<td></td>
<td>ENDIF;</td>
</tr>
<tr>
<td></td>
<td>ENDIF;</td>
</tr>
<tr>
<td></td>
<td>ELSE /* RTCP IP flow(s) */</td>
</tr>
<tr>
<td></td>
<td>IF bAS=AS:&lt;bandwidth&gt; and bAS=RSS:&lt;bandwidth&gt; is present THEN</td>
</tr>
<tr>
<td></td>
<td>Max_BW_UL:= (bAS + bRS) / 1000;</td>
</tr>
<tr>
<td></td>
<td>Max_BW_DL:= (bAS + bRS) / 1000;</td>
</tr>
<tr>
<td></td>
<td>ELSE</td>
</tr>
<tr>
<td></td>
<td>IF bAS=AS:&lt;bandwidth&gt; is present THEN</td>
</tr>
<tr>
<td></td>
<td>IF bAS=RSS:&lt;bandwidth&gt; is present and bAS=RR:&lt;bandwidth&gt; is not present THEN</td>
</tr>
<tr>
<td></td>
<td>Max_BW_UL:= MAX[0.05 * bAS, bRS / 1000];</td>
</tr>
</tbody>
</table>
Authorized access network QoS Parameter per flow identifier | Derivation from SDP Parameters (see NOTE 4)
---|---
Max_BW_DL := MAX[0.05 * bas, bRS / 1000];
ENDIF;
IF bas=RS: <bandwidth> is not present and bRR=RR: <bandwidth> is present THEN
Max_BW_DL := MAX[0.05 * bas, bRR / 1000];
Max_BW_DL := MAX[0.05 * bas, bRR / 1000];
ENDIF;
IF bas=RS: <bandwidth> and bRR=RR: <bandwidth> is not present THEN
Max_BW_DL := 0.05 * bas;
Max_BW_DL := 0.05 * bas;
ENDIF;
ELSE
Max_BW_UL := as set by the UE manufacture;
Max_BW_DL := as set by the UE manufacture;
ENDIF;
ENDIF;
ELSE
No authorization is done;
ENDIF;

Maximum Authorized QoS Class Identifier [QCI] per flow identifier (see NOTE 1, 2 and 3)

IF SBC is applied THEN
IF (all media IP flows of media type "audio" or "video" for the session are unidirectional and have the same direction) THEN
MaxService := 3 or 4;
ELSE
MaxService := 1 or 2;
ENDIF;
CASE <media> OF
"audio": QCI := MaxService;
"video": QCI := MaxService;
"application": QCI := 1 or 2;
"data": QCI := 6 or 7 or 8;
"control": QCI := 5;
/*new media type*/
OTHERWISE: QCI := 9;
END;
ELSE
No authorization is done;
ENDIF;

NOTE 1: The Maximum Authorized Traffic Class for a RTCP IP flow is the same as for the corresponding RTP media IP flow.
NOTE 2: When audio or video IP flow(s) are removed from a session, the parameter MaxService shall keep the originally assigned value.
NOTE 3: When audio or video IP flow(s) are added to a session, the UE shall derive the parameter MaxService taking into account the already existing media IP flows within the session
NOTE 4: The SDP parameters are described in [8].
NOTE 5: The 'b=RS:' and 'b=RR:' SDP bandwidth modifiers are defined in [6].

The UE should, per ongoing session, store the authorized access network QoS parameters per flow identifier.
Before it activates or modifies a bearer, the UE should check that the requested Guaranteed Bitrate UL/DL (if the Traffic Class is Conversational or Streaming) or the requested Maximum Bitrate UL/DL (if the Traffic Class is Interactive or Background) does not exceed the Maximum Authorized Bandwidth UL/DL per bearer (calculated according to the rule in table A.3.3.2). If the requested Guaranteed Bitrate UL/DL or the requested Maximum Bitrate UL/DL exceeds the Maximum Authorized Bandwidth UL/DL per bearer, the UE should reduce the requested Guaranteed Bitrate UL/DL or the requested Maximum Bitrate UL/DL to the Maximum Authorized Bandwidth UL/DL per bearer. Furthermore, if the rule in table A.3.3.1 for calculating QCI per flow identifier is implemented, the UE should check that the requested access network QoS parameter Traffic Class does not exceed the Traffic Class.
Class corresponding to QCI per bearer (calculated according to the rule in table A.3.3.2). If the requested access network QoS parameter Traffic Class exceeds the Maximum Authorized Traffic Class corresponding to QCI per bearer, the UE should reduce the requested access network QoS parameter Traffic Class to the Maximum Authorized Traffic Class corresponding to the QCI per bearer.

Table A.3.3.2: Rules for calculating the Maximum Authorized Bandwidths and Maximum Authorized Traffic Class per bearer in the UE

<table>
<thead>
<tr>
<th>Authorized access network QoS Parameter per bearer</th>
<th>Calculation Rule</th>
</tr>
</thead>
</table>
| Maximum Authorized Bandwidth DL and UL per bearer | IF SBBC is applied THEN  
Maximum Authorized Bandwidth DL/UL per bearer is the sum of all Maximum Authorized Bandwidth DL/UL for all the flow identifiers associated with that bearer;  
ELSE  
No authorization is done;  
ENDIF; |
| QCI per bearer | IF SBBC is applied THEN  
QCI = MAX [QoS parameters needed per flow identifier among all the flow identifiers associated with that bearer];  
ELSE  
No authorization is done;  
ENDIF; |
Annex B (normative): Flow identifiers: Format definition and examples

B.1 Format of a flow identifier

A flow identifier is expressed as a 2-tuple as follows:

\[
\langle \text{The ordinal number of the position of the media component description in the SDI}, \text{The ordinal number of the IP flow(s) within the media component description assigned in the order of increasing uplink port numbers as detailed below} \rangle
\]

where both are numbered starting from 1.

If UE and AF share an algorithm for a given application, which guarantees that UE and AF assign the same ordinal number to each media component, the ordinal numbers of the IP Flows within a media component shall be assigned according to the following rules:

- All IP flow(s) or bidirectional combinations of two IP flow(s) within the media component, for which an uplink destination port number is available, shall be assigned ordinal numbers in the order of uplink destination port numbers.
- All IP flows, where no uplink destination port number is available, shall be assigned the next higher ordinal numbers in the order of downlink destination port numbers.

The ordinal number of a media component shall not be changed when the session description information is modified.

For SDP, the flow identifier shall be assigned in the following way:

<table>
<thead>
<tr>
<th>The ordinal number of the position of the &quot;m=&quot; line in the SDP</th>
<th>The ordinal number of the IP flow(s) within the &quot;m=&quot; line assigned in the order of increasing uplink destination port numbers, if uplink destination port numbers are available. For downlink or inactive unicast media IP flows, an uplink destination port number is nevertheless available, if SDP offer-answer according to [9] is used.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>The ordinal number of the IP flow(s) within the &quot;m=&quot; line assigned in the order of increasing downlink destination port numbers, if no uplink destination port numbers are available.</td>
</tr>
</tbody>
</table>

51
If no SDI with fixed and unique positions for media components is exchanged between UE and AF, the UE and AF may assign the ordinal numbers of the media components in another application-dependent algorithm which guarantees that UE and AF assign the same ordinal number to each media component.

If UE and AF do not share an algorithm for a given application, which guarantees that UE and AF assign the same ordinal number to each media component, the ordinal number of the media component shall be set to zero and the ordinal number of the IP flows shall be assigned according to the following rules:

1. If ordinal numbers for several IP flows are assigned at the same time, all uplink IP flows shall be assigned lower ordinal number than all downlink IP flows.

2. If ordinal numbers for several IP flows are assigned at the same time, all uplink and all downlink IP flows shall separately be assigned ordinal numbers according to increasing internet protocol number assigned by IANA (e.g. 8 for TCP and 17 for UDP)

3. If ordinal numbers for several IP flows are assigned at the same time, for each internet protocol with a port concept, all uplink and all downlink IP flows of this internet protocol shall separately be assigned ordinal numbers according to increasing port numbers.

4. If IP flows are removed from an existing session, the previously assigned binding info shall remain unmodified for the remaining IP flows.

5. If IP flows are added to an existing session, the previously assigned binding info shall remain unmodified and the new IP flows shall be assigned ordinal numbers following the rules 1. to 3., starting with the first previously unused ordinal number. The numbers freed in step 4. shall not be reused.

### B.2 Example 1

An UE, as the offerer, sends a SDP session description, as shown in table A.1, to an AF (only relevant SDP parameters are shown):

<table>
<thead>
<tr>
<th>Table B.1: The values of the SDP parameters sent by the UE in example 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>v=0</td>
</tr>
<tr>
<td>o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A</td>
</tr>
<tr>
<td>s=MM01</td>
</tr>
<tr>
<td>i=One unidirectional audio media and one unidirectional video media and one bidirectional application media</td>
</tr>
<tr>
<td>t=3262377600 3262809600</td>
</tr>
<tr>
<td>m=video 50230 RTP/AVP 31</td>
</tr>
<tr>
<td>c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A</td>
</tr>
<tr>
<td>a=recvonly</td>
</tr>
<tr>
<td>m=audio 50330 RTP/AVP 0</td>
</tr>
<tr>
<td>c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A</td>
</tr>
<tr>
<td>a=sendonly</td>
</tr>
<tr>
<td>m=application 50430 udp wb</td>
</tr>
<tr>
<td>c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A</td>
</tr>
<tr>
<td>a=sendrecv</td>
</tr>
</tbody>
</table>

and receives the SDP parameters, as shown in table B.2, from the AF:

<table>
<thead>
<tr>
<th>Table B.2: The values of the SDP parameters sent by the AF in example 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>v=0</td>
</tr>
<tr>
<td>o=ecsreid 3262464865 3262464868 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A</td>
</tr>
</tbody>
</table>

52
From this offer–answer exchange of SDP parameters the UE and the PCRF each creates a list of flow identifiers comprising the IP flows as shown in table B.3:

<table>
<thead>
<tr>
<th>Order of</th>
<th>Type of IP flows</th>
<th>Destination IP address / Port number of the IP flows</th>
<th>Flow identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RTP (Video) DL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50230</td>
<td>&lt;1,1&gt;</td>
</tr>
<tr>
<td>1</td>
<td>RTCP DL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50231</td>
<td>&lt;1,2&gt;</td>
</tr>
<tr>
<td>1</td>
<td>RTCP UL</td>
<td>2001:0646:00A0:03A7:02D0:59FF:FE40:2014 / 51373</td>
<td>&lt;1,2&gt;</td>
</tr>
<tr>
<td>2</td>
<td>RTP (Audio) UL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50331</td>
<td>&lt;2,1&gt;</td>
</tr>
<tr>
<td>2</td>
<td>RTCP DL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50331</td>
<td>&lt;2,2&gt;</td>
</tr>
<tr>
<td>2</td>
<td>RTCP UL</td>
<td>2001:0646:00A0:03A7:02D0:59FF:FE40:2014 / 49171</td>
<td>&lt;2,2&gt;</td>
</tr>
<tr>
<td>3</td>
<td>UDP (application) DL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50430</td>
<td>&lt;3,1&gt;</td>
</tr>
<tr>
<td>3</td>
<td>UDP (application) UL</td>
<td>2001:0646:00A0:03A7:02D0:59FF:FE14:F33A / 32416</td>
<td>&lt;3,1&gt;</td>
</tr>
</tbody>
</table>

### B.3 Example 2

In the general case, multiple ports may be specified with a "number of ports" qualifier as follows:

\[
m=<\text{media}> <\text{port}>/\text{number of ports} <\text{transport}> <\text{fmt list}>
\]

An UE, as the offerer, sends a SDP session description, as shown in table B.4, to an AF (only relevant SDP parameters are shown):

<table>
<thead>
<tr>
<th>Order of</th>
<th>Type of IP flows</th>
<th>Destination IP address / Port number of the IP flows</th>
<th>Flow identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>v=0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o=ecsreid 3262464321 3262464325 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s=MM02</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i=One unidirectional audio media consisting of two media IP flows described by one media component</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>t=3262377600 3262809600</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>m=audio 50330/2 RTP/AVP 0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c=IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>a=recvonly</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
and receives the SDP parameters, as shown in table B.5, from the AF:

**Table B.5: The values of the SDP parameters sent by the AF in example 2.**

<table>
<thead>
<tr>
<th>v=0</th>
</tr>
</thead>
<tbody>
<tr>
<td>o=ecsreid 3262464321 3262464325 IN IP6 2001:0646:00F1:0045:02D0:59FF:FE14:F33A</td>
</tr>
<tr>
<td>s=MM02</td>
</tr>
<tr>
<td>i=One unidirectional audio media consisting of two media IP flows described by one media component</td>
</tr>
<tr>
<td>t=3262377600 3262809600</td>
</tr>
<tr>
<td>m=audio 49170/2 RTP/AVP 0</td>
</tr>
<tr>
<td>c=IN IP6 2001:0646:000A:03A7:02D0:59FF:FE40:2014</td>
</tr>
<tr>
<td>a=sendonly</td>
</tr>
</tbody>
</table>

From this offer–answer exchange of SDP parameters the UE and the PCRF each creates a list of flow identifiers comprising the IP flows as shown in table B.6:

**Table B.6: Flow identifiers in example 2.**

<table>
<thead>
<tr>
<th>Order of 'm='-line</th>
<th>Type of IP flows</th>
<th>Destination IP address / Port number of the IP flows</th>
<th>Flow identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>RTP (audio) DL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50330</td>
<td>&lt;1,1&gt;</td>
</tr>
<tr>
<td>1</td>
<td>RTCP DL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50331</td>
<td>&lt;1,2&gt;</td>
</tr>
<tr>
<td>1</td>
<td>RTCP UL</td>
<td>2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 49171</td>
<td>&lt;1,2&gt;</td>
</tr>
<tr>
<td>1</td>
<td>RTP (audio) DL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50332</td>
<td>&lt;1,3&gt;</td>
</tr>
<tr>
<td>1</td>
<td>RTCP DL</td>
<td>2001:0646:00F1:0045:02D0:59FF:FE14:F33A / 50333</td>
<td>&lt;1,4&gt;</td>
</tr>
<tr>
<td>1</td>
<td>RTCP UL</td>
<td>2001:0646:000A:03A7:02D0:59FF:FE40:2014 / 49173</td>
<td>&lt;1,4&gt;</td>
</tr>
</tbody>
</table>
Annex C (normative):
Support for SIP forking

C.1 Support for SIP forking

The P-CSCF shall be able to handle forking when SBBC is applied. Forking can occur as specified in 3GPP2 MMD [12]. The related UE procedures are described in [12].

C.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. Multiple early dialogs may be established during this process.

The UE and the P-CSCF become aware of the forking only when a subsequent provisional response arrives for a new early dialog, although early media may be exchanged prior to receipt of SDP from the answerer. After the first SDP response is received, for each subsequent provisional response containing an SDP response, the P-CSCF may 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 PCRF shall identify the existing authorization information for that AF session. The PCRF may send additional PCC Rules as required by the Flow Description AVPs within the session information to the AGW. The PCRF may authorize any additional media components and any increased QoS requirements for the previously authorized media components, as requested within the service information. The PCRF may authorize the maximum bandwidth according to local policy. By default this is the maximum bandwidth required by any of the dialogs, but not the sum of the bandwidths required by all dialogs. 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.

C.1.2 Updating the authorization information at the final answer

The P-CSCF shall store the SDP information for each early dialog separately until the first final SIP answer is received. Then the related early dialog is progressed to an established dialog to establish the final SIP session. All the other early dialogues are terminated. The service 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 PCRF shall update installed PCC Rules information and Authorized-QoS information to match only the requirements of the service information within this AA request. The PCRF should immediately remove PCC Rule(s) not matching IP flow(s) in the updated Service Information, to reduce the risk for initial clipping of the media stream, and to minimize possible misuse of resources.