ETSI TS 129 212 V8.2.0 (2009-02)

Technical Specification

Universal Mobile Telecommunications System (UMTS);
LTE;
Policy and charging control over Gx reference point
(3GPP TS 29.212 version 8.2.0 Release 8)

Reference
RTS/TSGC-0329212v820

Keywords
LTE, UMTS

ETSI

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

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

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

Intellectual Property Rights

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

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

Foreword

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

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

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

Contents

Foreword

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

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

Version x.y.z

where:

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

1 Scope

The present document provides the stage 3 specification of the Gx and Gxx reference points for the present release. The functional requirements and the stage 2 specifications of the Gx and Gxx reference point are contained in 3GPP TS 23.203 [7]. The Gx reference point lies between the Policy and Charging Rule Function and the Policy and Charging Enforcement Function. The Gxx reference point lies between the Policy and Charging Rule Function and the Bearer Binding and Event Reporting Function.

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

2 References

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

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

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

[2] 3GPP TS 29.210: "Charging Rule Provisioning over Gx Interface".

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

[4] 3GPP TS 29.208: "End-to-end Quality of Service (QoS) signalling flows".

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

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

[7] 3GPP TS 23.203: "Policy Control and Charging architecture".

[8] 3GPP TS 29.213: "Policy and charging control signalling flows and Quality of Service (QoS) parameter mapping".

[9] IETF RFC 4006: "Diameter Credit Control Application".

[10] 3GPP TS 29.214: "Policy and Charging Control over Rx reference point".

[11] 3GPP TS 29.061: "Interworking between the Public Land Mobile Network (PLMN) supporting packet based services and Packet Data Networks (PDN)".

[12] IETF RFC 4005: "Diameter Network Access Server Application".

[13] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification".

[14] 3GPP TS 29.229: "Cx and Dx interfaces based on Diameter protocol; Protocol details".

[15] IETF RFC 3162: "Radius and IPv6".

[16] 3GPP TS 32.295: "Telecommunication management; Charging management; Charging Data Record (CDR) transfer".

[17] 3GPP TS 23.060: "General Packet Radio Service (GPRS); Service description; Stage 2".

[18] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[19] 3GPP TS 32.299: "Telecommunication management; Charging management; Diameter charging applications ".

[20] 3GPP2 X.S0011-D: "cdma2000 Wireless IP Network Standard".

[21] 3GPP TS 32.240: "Telecommunication management; Charging management; Charging architecture and principles".

[22] 3GPP TS 29.274: '3GPP Evolved Packet System. Evolved GPRS Tunnelling Protocol for EPS (GTPv2)

[23] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

3 Definitions and abbreviations

3.1 Definitions

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

IP-CAN bearer: IP transmission path of defined capacity, delay and bit error rate, etc.
See 3GPP TS 21.905 [1] for the definition of bearer.

IP-CAN session: association between a UE and an IP network
The association is identified by one or more UE IP addresses (one IPv4 and/or one IPv6 address) together with a UE identity information, if available, and a PDN represented by a PDN ID (e.g. an APN). An IP-CAN session incorporates one or more IP-CAN bearers. Support for multiple IP-CAN bearers per IP-CAN session is IP-CAN specific. An IP-CAN session exists as long as the related UE IP addresses are assigned and announced to the IP network.

IP flow: unidirectional flow of IP packets with the same source IP address and port number and the same destination IP address and port number and the same transport protocol
Port numbers are only applicable if used by the transport protocol.

3.2 Abbreviations

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

AF	Application Function
BBERF	Bearer Binding and Event Reporting Function
OCS	Online charging system
OFCS	Offline charging system
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rule Function

4 Gx reference point

4.1 Overview

The Gx reference point is located between the Policy and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF). The Gx reference point is used for provisioning and removal of PCC rules from the PCRF to the PCEF and the transmission of traffic plane events from the PCEF to the PCRF. The Gx reference point can be used for charging control, policy control or both by applying AVPs relevant to the application.

The stage 2 level requirements for the Gx reference point are defined in 3GPP TS 23.203 [7].

Signalling flows related to the both Rx and Gx interfaces are specified in 3GPP TS 29.213 [8].

4.2 Gx Reference model

The Gx reference point is defined between the PCRF and the PCEF. The relationships between the different functional entities involved are depicted in figure 4.1.

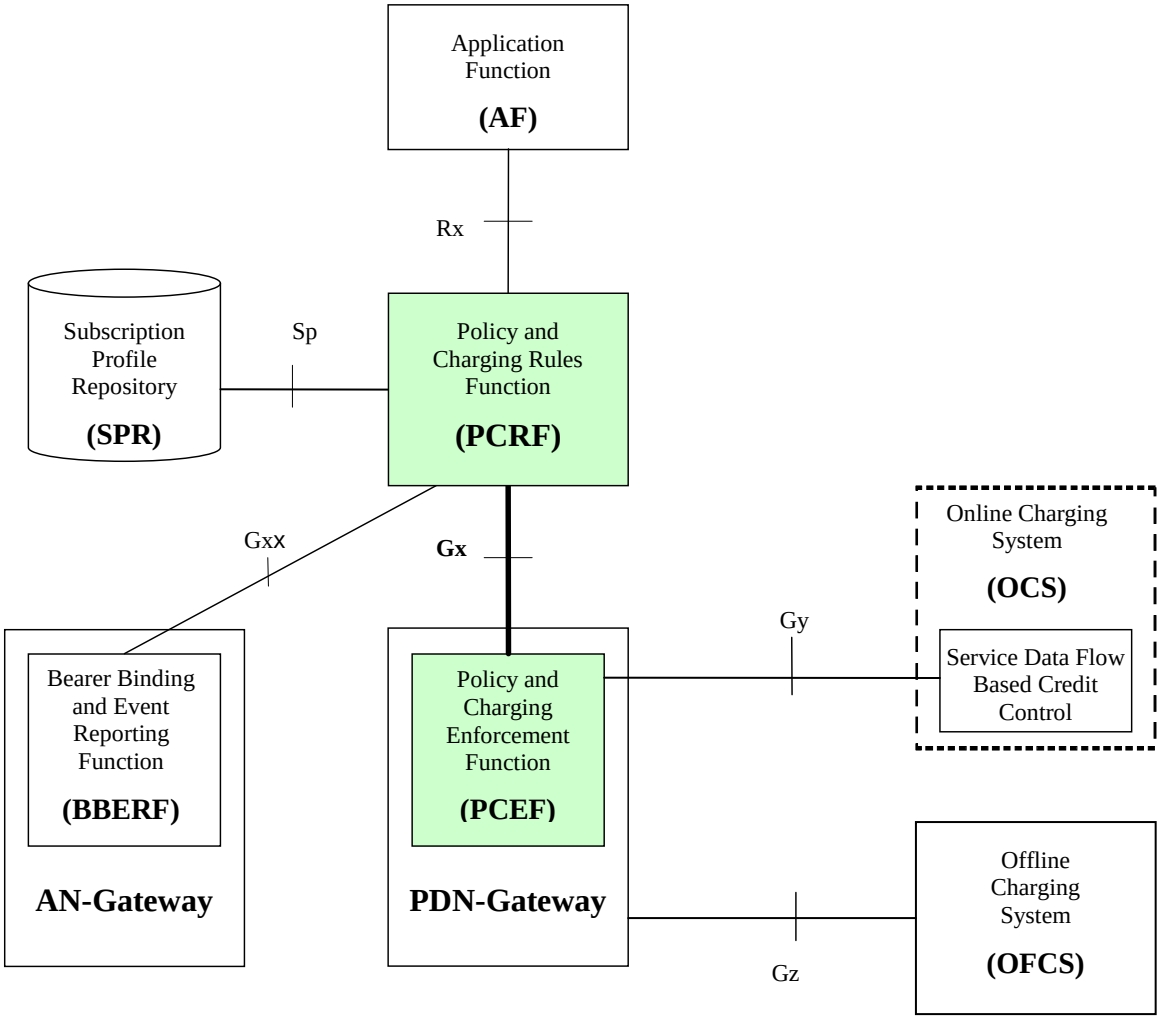

Figure 4.1: Gx reference point at the Policy and Charging Control (PCC) architecture

NOTE: The details associated with the Sp reference point are not specified in this Release. The SPR"s relation to existing subscriber databases is not specified in this Release.

4.3 PCC Rules

4.3.1 PCC Rule Definition

The purpose of the PCC rule is to:

- Detect a packet belonging to a service data flow.
  - The service data flow filters within the PCC rule are used for the selection of downlink IP CAN bearers.
  - The service data flow filters within the PCC rule are used for the enforcement that uplink IP flows are transported in the correct IP CAN bearer.

- Identify the service the service data flow contributes to.
- Provide applicable charging parameters for a service data flow.
- Provide policy control for a service data flow.

The PCEF shall select a PCC rule for each received packet by evaluating received packets against service data flow filters of PCC rules in the order of the precedence of the PCC rules.. When a packet matches a service data flow filter, the packet matching process for that packet is completed, and the PCC rule for that filter shall be applied.

There are two different types of PCC rules as defined in [7]:

- Dynamic PCC rules. Dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be activated, modified and deactivated at any time.
- Predefined PCC rules. Preconfigured in the PCEF. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

NOTE: The operator may define a predefined PCC rule, to be activated by the PCEF. Such a predefined rule is not explicitly known in the PCRF.

A PCC rule consists of:

- a rule name;
- service identifier;
- service data flow filter(s);
- precedence;
- gate status;
- QoS parameters;
- charging key (i.e. rating group);
- other charging parameters.

The rule name shall be used to reference a PCC rule in the communication between the PCEF and the PCRF.

The service identifier shall be used to identify the service or the service component the service data flow relates to.

The service flow filter(s) shall be used to select the traffic for which the rule applies.

The gate status indicates whether the service data flow, detected by the service data flow filter(s), may pass (gate is open) or shall be discarded (gate is closed) in uplink and/or in downlink direction.

The QoS information includes the QoS class identifier (authorized QoS class for the service data flow) , the Allocation and Retention Priority (ARP) and authorized bitrates for uplink and downlink.

The charging parameters define whether online and offline charging interfaces are used, what is to be metered in offline charging, on what level the PCEF shall report the usage related to the rule, etc.

For different PCC rules with overlapping service data flow filter, the precedence of the rule determines which of these rules is applicable. When a dynamic PCC rule and a predefined PCC rule have the same precedence, the dynamic PCC rule takes precedence.

PCC rule also includes Application Function record information for enabling charging correlation between the application and bearer layer if the AF has provided this information via the Rx interface. For IMS this includes the IMS Charging Identifier (ICID) and flow identifiers.

4.3.2 Operations on PCC Rules

For dynamic PCC rules, the following operations are available:

- Installation: to provision a PCC rules that has not been already provisioned.
- Modification: to modify a PCC rule already installed.
- Removal: to remove a PCC rule already installed.

For predefined PCC rules, the following operations are available:

- Activation: to allow the PCC rule being active.
- Deactivation: to disallow the PCC rule.

The procedures to perform these operations are further described in clause 4.5.2.

4.4 Functional elements

4.4.1 PCRF

The PCRF (Policy Control and Charging Rules Function) is a functional element that encompasses policy control decision and flow based charging control functionalities. These 2 functionalities are the heritage of the release 6 logical entities PDF and CRF respectively. The PCRF provides network control regarding the service data flow detection, gating, QoS and flow based charging (except credit management) towards the PCEF. The PCRF receives session and media related information from the AF and informs AF of traffic plane events.

The PCRF shall provision PCC Rules to the PCEF via the Gx reference point. Particularities for the Gxx reference point are specified in clause 4a.4.1.

The PCRF PCC Rule decisions may be based on one or more of the following:

- Information obtained from the AF via the Rx reference point, e.g. the session, media and subscriber related information.
- Information obtained from the PCEF via the Gx reference point, e.g. IP-CAN bearer attributes, request type and subscriber related information.
- Information obtained from the SPR via the Sp reference point, e.g. subscriber and service related data.

NOTE: The details associated with the Sp reference point are not specified in this Release. The SPR"s relation to existing subscriber databases is not specified in this Release.

- Information obtained from the BBERF via the Gxx reference point.
- Own PCRF pre-configured information.

If the information from the PCEF contains traffic mapping information not matching any service data flow filter known to the PCRF, and the PCRF allows the UE to request enhanced QoS for services not known to the PCRF, the PCRF shall add this traffic mapping information as service data flow filters to the corresponding authorized PCC Rule. The PCRF may wildcard missing filter parameters, e.g. missing uplink TFT address and port information in case of GPRS.

The PCRF shall report events to the AF via the Rx reference point.

The PCRF shall inform the PCEF through the use of PCC rules on the treatment of each service data flow that is under PCC control, in accordance with the PCRF policy decision(s

The PCRF shall be able to select the bearer control mode that will apply for the IP-CAN session and provide it to the PCEF via the Gx reference point.

Upon subscription to loss of AF signalling bearer notifications by the AF, the PCRF shall request the PCEF to notify the PCRF of the loss of resources associated to the PCC Rules corresponding with AF Signalling IP Flows, if this has not been requested previously.

4.4.2 PCEF

The PCEF (Policy and Charging Enforcement Function) is the functional element that encompasses policy enforcement and flow based charging functionalities. These 2 functionalities are the heritage of the release 6 logical entities PEP and TPF respectively. This functional entity is located at the Gateway (e.g. GGSN in the GPRS case, and PDG in the WLAN case). It provides control over the user plane traffic handling at the Gateway and its QoS, and provides service data flow detection and counting as well as online and offline charging interactions.

For a service data flow that is under policy control the PCEF shall allow the service data flow to pass through the Gateway if and only if the corresponding gate is open.

For a service data flow that is under charging control the PCEF shall allow the service data flow to pass through the Gateway if and only if there is a corresponding active PCC rule and, for online charging, the OCS has authorized the applicable credit with that Charging key. The PCEF may let a service data flow pass through the Gateway during the course of the credit re-authorization procedure.

If requested by the PCRF, the PCEF shall report to the PCRF when the status of the related service data flow changes. This procedure can be used to monitor an IP-CAN bearer dedicated for AF signalling traffic.

In case the SDF is tunnelled at the BBERF, the PCEF shall inform the PCRF about the mobility protocol tunnelling header of the service data flows at IP-CAN session establishment.

4.5 PCC procedures over Gx reference point

4.5.1 Request for PCC rules

The PCEF shall indicate, via the Gx reference point, a request for PCC rules in the following instances.

1) At IP-CAN session establishment:

   - The PCEF shall send a CC-Request with CC-Request-Type AVP set to the value "INITIAL_REQUEST". The PCEF shall supply user identification and other attributes to allow the PCRF to identify the rules to be applied. The other attributes shall include the type of IP-CAN, the type of the radio access technology (e.g UTRAN, GERAN, WLAN) and the UE IP address. The PCEF may also include the Access-Network-Charging-Address and Access-Network-Charging-Identifier-Gx AVPs in the CC-Request. Furthermore, if the UE and the network support the network network-initiated bearer request procedure, the PCEF shall indicate this by supplying the Network Request Support AVP. If the UE indicated a preferred bearer control mode, the PCEF shall indicate this mode within the Bearer-Control Mode AVP.

     For IP-CAN types that support multiple IP-CAN bearers, the PCEF may provide the Default-EPS-Bearer-QoS AVP including the ARP and QCI values corresponding to the Default EPS Bearer QoS.

     For IP-CAN types that support multiple IP-CAN bearers, the PCEF shall provide the Bearer-Identifier AVP at the IP-CAN session establishment. In this case, the PCEF shall also include the Bearer-Operation AVP set to the value "Establishment".

     For 3GPP-EPS and 3GPP2 accesses, the PCEF shall provide the IP address(es) (IPv4 or IPv6, if available) of the SGW/AGW within the AN-GW-Address AVP.

2) At IP-CAN session modification:

   IP-CAN session modification with PCEF-requested rules can occur in the following cases:

   - When a new IP-CAN bearer is being established by the UE in an already existing IP-CAN Session.
   - When an IP-CAN bearer is being modified and an Event trigger is met.
   - When a n IP-CAN bearer is being terminated.

   The PCEF shall send a CC-Request with CC-Request-Type AVP set to the value "UPDATE_REQUEST". The PCEF may include the Access-Network-Charging-Address and Access-Network-Charging-Identifier-Gx

AVPs in the CC-Request. For an IP-CAN Session modification where an existing IP-CAN Bearer is modified, the PCEF shall supply within the PCC rule request the specific event which caused the IP-CAN session modification (within the Event-Trigger AVP) and any previously provisioned PCC rule(s) affected by the IP-CAN session modification. The PCC rules and their status shall be supplied to PCRF within the Charging-Rule-Report AVP.

In the case the PCRF performs the bearer binding and:

- a new IP-CAN bearer is being established, the PCEF shall assign a new bearer identifier to this IP-CAN bearer, include this identifier within the Bearer-Identifier AVP, and include the Bearer-Operation AVP set to the value "Establishment", and supply QoS related information as detailed in Clause 4.5.5.0a;

- an existing IP-CAN bearer is being modified, the PCEF shall include the Bearer-Identifier AVP and the Bearer-Operation AVP set to the value "Modification", and supply QoS related information as detailed in Clause 4.5.5.0a. If the Event trigger that caused the IP-CAN bearer modification applies at session level (i.e. it is common to all the bearers belonging to that IP-CAN session), PCEF shall send a single CC-Request for all the affected bearers. In this case, the Bearer-Identifier AVP shall not be included to indicate that it applies to all the IP-CAN bearers in the IP-CAN session.

In the case both the PCRF and the PCEF may performs the bearer binding:

- If the UE request the establishment of a new IP-CAN bearer, the PCEF shall assign a new bearer identifier to this IP-CAN bearer, include this identifier within the Bearer-Identifier AVP, and include the Bearer-Operation AVP set to the value "Establishment", the UE-provided TFT filters and the requested QoS of the new IP-CAN bearer and further QoS related information as detailed in Clause 4.5.5.0a.

- If an existing IP-CAN bearer is being modified:

  - If the PCEF has not yet notified the PCRF about this IP CAN bearer and the UE assigns one or more Traffic Flow template(s) within an IP CAN Bearer modification request, the PCEF shall assign a new bearer identifier to this IP-CAN bearer, and shall include the Bearer-Identifier AVP and the Bearer-Operation AVP set to the value "Establishment", the UE-provided TFT filters and the requested QoS of the new IP-CAN bearer and further QoS related information as detailed in Clause 4.5.5.0a. The PCEF shall modify the received requested QoS by removing the bandwidth required for PCC rules the PCEF has previously bound to this IP CAN bearer and indicate this modified requested QoS to the PCRF.

NOTE: The details how the bandwidth required for PCC rules the PCEF has previously bound to this IP CAN bearer are calculated are ffs, e.g. the significance of the maximum and guaranteed bandwidth per PCC rule in this calculation.

  - If the PCEF has already notified the PCRF about this IP CAN bearer, the PCEF shall include the Bearer-Identifier AVP and the Bearer-Operation AVP set to the value "Modification" and QoS related information as detailed in Clause 4.5.5.0a. If the PCEF has received a new requested QoS as part of an IP CAN bearer modification request, the PCEF shall modify this received requested QoS by removing the bandwidth required for PCC rules the PCEF has previously bound to this IP CAN bearer and indicate this modified requested QoS to the PCRF.

NOTE: The details how the bandwidth required for PCC rules the PCEF has previously bound to this IP CAN bearer are calculated are ffs, e.g. the significance of the maximum and guaranteed bandwidth per PCC rule in this calculation.

If the Event trigger that caused the IP-CAN bearer modification applies at session level (i.e. it is common to all the bearers belonging to that IP-CAN session), PCEF shall send a single CC-Request for all the affected bearers. In this case, the Bearer-Identifier AVP shall not be included to indicate that it applies to all the IP-CAN bearers in the IP-CAN session. If the Event trigger that caused the IP CAN bearer modification applies at bearer level, the Charging-Rule-Report AVP shall include all the affected PCC rules.

PCC rules can also be requested as a consequence of a failure in the PCC rule installation/activation or enforcement without requiring an Event-Trigger. See clause 4.5.12.

If the PCRF is, due to incomplete, erroneous or missing information (e.g. QoS, SGSN address, RAT type, TFT, subscriber information) not able to provision a policy decision as response to the request for PCC rules by the PCEF, the PCRF may reject the request using a CC Answer with the Gx experimental result code DIAMETER_ERROR_INITIAL_PARAMETERS (5140). If the PCEF receives a CC Answer with this code, the PCEF shall reject the IP-CAN session establishment or modification that initiated the CC Request.

If the PCRF does not accept one or more of the traffic mapping filters provided by the PCEF in a CC Request (e.g. because the PCRF does not allow the UE to request enhanced QoS for services not known to the PCRF), the PCRF shall reject the request using a CC Answer with the Gx experimental result code DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED (5144). If the PCEF receives a CC Answer with this code, the PCEF shall reject the IP-CAN session establishment or modification that initiated the CC Request.

4.5.2 Provisioning of PCC rules

The PCRF shall indicate, via the Gx reference point, PCC rules to be applied at the PCEF. This may be using one of the following procedures:

- PULL procedure(Provisioning solicited by the PCEF): In response to a request for PCC rules being made by the PCEF, as described in the preceding section, the PCRF shall provision PCC rules in the CC-Answer; or

- PUSH procedure(Unsolicited provisioning): The PCRF may decide to provision PCC rules without obtaining a request from the PCEF, e.g. in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision PCC rules without a request from the PCEF, the PCRF shall include these PCC rules in an RA-Request message. No CCR/CCA messages are triggered by this RA-Request.

For each request from the PCEF or upon the unsolicited provision the PCRF shall provision zero or more PCC rules.. The PCRF may perform an operation on a single PCC rule by one of the following means:

- To activate or deactivate a PCC rule that is predefined at the PCEF, the PCRF shall provision a reference to this PCC rule within a Charging-Rule-Name AVP and indicate the required action by choosing either the Charging-Rule-Install AVP or the Charging-Rule-Remove AVP.

- To install or modify a PCRF-provisioned PCC rule, the PCRF shall provision a corresponding Charging-Rule-Definition AVP within a Charging-Rule-Install AVP.

- To remove a PCC rule which has previously been provisioned by .the PCRF, the PCRF shall provision the name of this rule as value of a Charging-Rule-Name AVP within a Charging-Rule-Remove AVP.

- If the PCRF performs the bearer binding, the PCRF may move previously installed or activated PCC rules from one IP CAN bearer to another IP CAN bearer, as described further down.

As an alternative to providing a single PCC rule, the PCRF may provide a Charging-Rule-Base-Name AVP within a Charging-Rule-Install AVP or the Charging-Rule-Remove AVP as a reference to a group of PCC rules predefined at the PCEF. With a Charging-Rule-Install AVP, a predefined group of PCC rules is activated or moved. With a Charging-Rule-Remove AVP, a predefined group of PCC rules is deactivated.

The PCRF may combine multiple of the above PCC rule operations in a single command.

To activate a predefined PCC rule at the PCEF, the rule name within a Charging-Rule-Name AVP shall be supplied within a Charging-Rule-Install AVP as a reference to the predefined rule. To activate a group of predefined PCC rules within the PCEF (e.g. gold users or gaming services) the PCC rule base name within a Charging-Rule-Base-Name AVP shall be supplied within a Charging-Rule-Install AVP as a reference to the group of predefined PCC rules. If the PCRF performs the bearer binding, the PCRF shall indicate the IP CAN bearer where the PCC rules shall be activated using a Bearer-Identifier AVP within the Charging-Rule-Install AVP.

To install a new or modify an already installed PCRF defined PCC rule, the Charging-Rule-Definition AVP shall be used. If a PCC rule with the same rule name, as supplied in the Charging-Rule-Name AVP within the Charging-Rule-Definition AVP, already exists at the PCEF, the new PCC rule shall update the currently installed rule. If the existing PCC rule already has attributes also included in the new PCC rule definition, the existing attributes shall be overwritten. Any attribute in the existing PCC rule not included in the new PCC rule definition shall remain valid.

If the PCRF performs the bearer binding and installs or activates a new PCC rule, the PCRF shall indicate the IP CAN bearer where the new rule shall be installed using a Bearer-Identifier AVP within the Charging-Rule-Install AVP. If the

PCRF modifies an already installed PCC rule, the PCRF does not need to indicate the bearer. If the PCEF obtains an updated definition of a PCC rule within a Charging-Rule-Install AVP without a Bearer-Identifier AVP, the PCEF shall continue to apply the PCC rule to the IP CAN bearer that has previously been indicated.

If the PCRF does not perform the bearer binding and installs or activates a new PCC rule, the PCRF does not indicate the bearer within the Charging-Rule-Install AVP. The PCEF shall then perform the bearer binding and select the IP CAN bearer where the provisioned new PCC rule is applied.

If the PCRF performs the bearer binding, the PCRF may move previously installed or activated PCC rule(s) from one IP CAN bearer to another IP CAN bearer. To move such PCC rule(s), the PCRF shall indicate the new bearer using the Bearer-Identifier AVP within a Charging-Rule-Install AVP and shall indicate the charging rules(s) to be moved using Charging-Rule name AVP(s), and/or a Charging-Rule-Base-Name AVP(s), and/or Charging-Rule-Definition AVP(s) (for PCC rule(s) that are modified at the same time). The PCEF shall then apply these PCC rules at the new indicated IP CAN bearer and shall remove them from the IP CAN bearer where the rules previously had been applied.

Further details of the binding mechanism can be found in 3GPP TS 29.213 [8].

For deactivating single predefined or removing PCRF-provided PCC rules, the Charging-Rule-Name AVP shall be supplied within a Charging-Rule-Remove AVP. For deactivating a group of predefined PCC rules, the Charging-Rule-Base-Name AVP shall be supplied within a Charging-Rule-Remove AVP.

NOTE: When deactivating a predefined PCC rule that is activated in more than one IP-CAN bearers, the predefined PCC rule is deactivated simultaneously in all the IP-CAN bearers where it was previously activated.

If the provisioning of PCC rules fails, the PCEF informs the PCRF as described in Clause 4.5.12 PCC Rule Error Handling. If network initiated procedures apply for the PCC rule and the corresponding IP-CAN bearer can not be established or modified to satisfy the bearer binding, then the PCEF shall reject the activation of a PCC rule using the Gx experimental result code DIAMETER_PCC_BEARER_EVENT and a proper Rule Failure Code. Depending on the cause, PCRF can decide if re-installation, modification, removal of PCC rules or any other action apply.

If the PCRF is unable to create a PCC rule for the response to the CC Request by the PCEF, the PCRF may reject the request as described in subclause 4.5.1.

4.5.2.1 Selecting a PCC rule for Uplink IP packets

If PCC is enabled, the PCEF shall select the applicable PCC rule for each received uplink IP packet within an IP CAN bearer by evaluating the packet against uplink service data flow filters of PCRF-provided or predefined active PCC rules of this IP CAN bearer in the order of the precedence of the PCC rules. When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the uplink service data flow filters of the PCRF-provided PCC rule shall be applied first. When a packet matches a service data flow filter, the packet matching process for that packet is completed, and the PCC rule for that filter shall be applied. Uplink IP packets which do not match any PCC rule of the corresponding IP CAN bearer shall be silently discarded.

4.5.2.2 Selecting a PCC rule and IP CAN Bearer for Downlink IP packets

If PCC is enabled, the PCEF shall select a PCC rule for each received downlink IP packet within an IP CAN session by evaluating the packet against downlink service data flow filters of PCRF-provided or predefined active PCC rules of all IP CAN bearers of the IP CAN session in the order of the precedence of the PCC rules. When a PCRF-provided PCC rule and a predefined PCC rule have the same precedence, the downlink service data flow filters of the PCRF-provided PCC rule shall be applied first. When a packet matches a service data flow filter, the packet matching process for that packet is completed, and the PCC rule for that filter shall be applied. The Downlink IP Packet shall be transported within the IP CAN bearer where the selected PCC rule is mapped. Downlink IP packets which do not match any PCC rule of the IP CAN session shall be silently discarded.

4.5.2.3 Gate function

The Gate Function represents a user plane function enabling or disabling the forwarding of service flow packets. A gate is described within a PCC rule. If the PCC rule contains Flow-Description AVP(s) applicable for uplink IP flows, it shall describe a gate for the corresponding uplink IP flows. If the PCC rule contains Flow-Description AVP(s) applicable for downlink IP flows, it shall describe a gate for the corresponding downlink IP flows. The Flow Status AVP of the PCC rule shall describe if the possible uplink and possible downlink gate is opened or closed.

The commands to open or close the gate shall lead to the enabling or disabling of the passage for corresponding IP packets. If the gate is closed all packets of the related IP flows shall be dropped. If the gate is opened the packets of the related IP flows are allowed to be forwarded.

4.5.2.4 Policy enforcement for "Authorized QoS" per PCC Rule

The PCRF can provide the authorized QoS for a PCC rule to the PCEF. The Provisioning of authorized QoS per PCC Rule shall be performed using the PCC rule provisioning procedure. For a PCRF-provided PCC rule, the "Authorized QoS" shall be encoded using a QoS-Information AVP within the Charging-Rule-Definition AVP of the PCC rule. If "Authorized QoS" is provided for a PCC rule, the PCEF shall enforce the corresponding policy.

See also Clause 4.5.5.

4.5.3 Provisioning of Event Triggers

The PCRF may provide one or several event triggers within one or several Event-Trigger AVP to the PCEF using the PCC rule provision procedure. Event triggers may be used to determine which IP-CAN session modification or specific event causes the PCEF to re-request PCC rules. Although event trigger reporting from PCEF to PCRF can apply for an IP CAN session or bearer depending on the particular event, provisioning of event triggers will be done at session level. The Event-Trigger AVP may be provided in combination with the initial or subsequent PCC rule provisioning.

The PCRF may add new event triggers or remove the already provided ones at each request from the PCEF or upon the unsolicited provision from the PCRF. In order to do so, the PCRF shall provide the new complete list of applicable event triggers including the needed provisioned Event-Trigger AVPs in the CCA or RAR commands.

The PCRF may remove all previously provided event triggers by providing the Event-Trigger AVP set to the value NO_EVENT_TRIGGERS. When an Event-Trigger AVP is provided with this value, no other Event-Trigger AVP shall be provided in the CCA or RAR command. Upon reception of an Event-Trigger AVP with this value, the PCEF shall not inform PCRF of any event.

If no Event-Trigger AVP is included in a CCA or RAR operation, any previously provisioned event trigger will be still applicable.

There are event triggers that are required to be unconditionally reported from the PCEF to the PCRF as specified in clause 5.3.7 eventhough the PCRF has not provisioned them to the PCEF.

4.5.4 Provisioning of charging related information for the IP-CAN session

4.5.4.1 Provisioning of Charging Addresses

In combination with the initial PCC rule provisioning only, the PCRF may provide OFCS and/or OCS addresses within a Charging-Information AVP to the PCEF defining the offline and online charging system addresses respectively. These shall overwrite any predefined addresses at the PCEF. Both primary and secondary addresses for OFCS and/or OCS shall be provided simultaneously. Provisioning OFCS or OCS addresses without PCC rules for offline or online charged service data flows, respectively, shall not be considered as an error since such PCC rules may be provided in later provisioning.

4.5.4.2 Provisioning of Default Charging Method

The default charging method indicates what charging method shall be used for every PCC rule where the charging method is omitted. The PCEF may have a pre-configured Default charging method.

Upon the initial interaction with the PCRF, the PCEF shall provide the pre-configured Default charging method if available within the Online AVP and/or Offline AVP embedded directly within the CCR command to the PCRF.

Upon the initial interaction with the PCEF, the PCRF may provide default charging method within the Online AVP or Offline AVP embedded directly within the CCA command to the PCEF. The default charging method provided by the PCRF shall overwrite any predefined default charging method at the PCEF.

4.5.5 Provisioning and Policy Enforcement of Authorized QoS

4.5.5.0 Overview

The PCRF may provide authorized QoS to the PCEF.

The authorized QoS shall be provisioned within a CCA or RAR Diameter message as QoS-Information AVP. The provisioning of the authorized QoS (which is composed of QCI, ARP and bitrates) is performed from the PCRF to the PCEF. The authorized QoS can refer to a PCC rule, to an IP CAN bearer, to a QCI or to an APN.

- When the authorized QoS applies to an IP CAN bearer, it shall be provisioned outside a Charging-Rule-Definition AVP and it shall also include the Bearer-Identifier AVP to indicate what bearer it applies to.
- When the authorized QoS applies to a PCC rule, it shall be provisioned within the corresponding PCC rule by including the QoS-Information AVP within the Charging-Rule-Definition AVP. The QoS-Information AVP shall not contain a Bearer-Identifier AVP.
- When the authorized QoS applies to QCI, authorised MBR per QCI is supplied. In such a case the authorized QoS shall be provisioned outside a Charging-Rule-Definition AVP at the command level.
- When the authorized QoS applies to an APN, authorised APN-Aggregate-Max-Bitrate UL/DL is supplied. In such a case the authorized QoS shall be provisioned outside a Charging-Rule-Definition AVP at command level. This case applies only for 3GPP-EPS access. See annex B for further details.
- When the authorized QoS applies to the default EPS bearer it shall be provisioned within the Default-EPS-Bearer-QoS AVP.

Authorized QoS at IP-CAN bearer level is access specific. See Annex A for further details.

The authorized QoS provides appropriate values for the resources to be enforced.

The authorized QoS for a PCC rule is a request for allocating the corresponding resources, and the authorized QoS for a QCI is a request for an upper limit for the MBR that the PCEF assigns to non-GBR bearers with that QCI.

The Provisioning of authorized QoS per PCC rule is a part of PCC rule provisioning procedure.

If the PCEF cannot allocate any of the resources as authorized by the PCRF, the PCEF should inform the PCRF using the Event-Trigger AVP with the corresponding value. If network initiated procedures apply for the PCC rule and the corresponding IP-CAN bearer can not be established or modified to satisfy the bearer binding, then the PCEF shall reject the activation of a PCC rule using the Gx experimental result code DIAMETER_PCC_BEARER_EVENT and a proper Event-Trigger value.

The PCEF is responsible for enforcing the policy based authorization.

QoS authorization information may be dynamically provisioned by the PCRF or it can be a pre-defined PCC rule in the PCEF.

The PCEF shall make sure that the total QoS information of the PCC rules for one IP-CAN bearer does not exceed the authorized QoS information, i.e. the information received from the PCRF.

If the PCRF is unable to make a decision for the response to the CC-Request by the PCEF, the PCRF may reject the request as described in subclause 4.5.1.

4.5.5.0a Provisioning of authorized QoS per IP CAN bearer

The authorized QoS per IP-CAN bearer is used if the bearer binding is performed by the PCRF (as defined in [8]). Provisioning of authorized QoS per IP-CAN bearer is access specific. See Annex A for further details.

4.5.5.1 Policy enforcement for authorized QoS per IP CAN bearer

The PCEF is responsible for enforcing the policy based authorization, i.e. to ensure that the requested QoS is in-line with the "Authorized QoS" per IP CAN Bearer. Policy enforcement of authorized QoS per IP-CAN bearer is access specific. See Annex A for further details.

4.5.5.2 Policy provisioning for authorized QoS per service data flow

The Provisioning of authorized QoS per service data flow is a part of PCC rule provisioning procedure, as described in Clause 4.5.2.

The authorized QoS per service data flow shall be provisioned within the corresponding PCC rule by including the QoS-Information AVP within the Charging-Rule-Definition AVP in the CCA or RAR commands. This QoS-Information AVP shall not contain a Bearer-Identifier AVP.

4.5.5.3 Policy enforcement for authorized QoS per service data flow

If an authorized QoS is defined for a PCC rule, the PCEF shall limit the data rate of the service data flow corresponding to that PCC rule not to exceed the maximum requested bandwidth for the PCC rule by discarding packets exceeding the limit.

The PCEF shall reserve the resources necessary for the guaranteed bitrate for the PCC rule upon receipt of a PCC rule provisioning including QoS information. For GBR bearers the PCEF should set the bearer"s GBR to the sum of the GBRs of all PCC rules that are active/installed and bound to that GBR bearer. For GBR bearers the PCEF should set the bearer"s MBR to the sum of the MBRs of all PCC rules that are active/installed and bound to that GBR bearer. For non-GBR bearers the PCEF may also set the bearer"s MBR to the sum of the MBRs of all PCC rules that are active and bound to that non-GBR bearer unless that sum exceeds a possibly provisioned authorized QoS per QCI for the bearer´s QCI (see Clause 4.5.5.6). If an authorized QoS per QCI has been provisioned for the bearer´s QCI, the PCEF should set the bearer"s MBR to the corresponding MBR. The access-specific BS Manager (as included in [8]) within the PCEF receives the authorised access-specific QoS information from the Translation/mapping function. Then the PCEF shall start the needed procedures to ensure that the provisioned resources are according to the authorized values. This may imply that the PCEF needs to request the establishment of new IP CAN bearer(s) or the modification of existing IP CAN bearer(s). If the enforcement is not successful, the PCEF shall inform the PCRF as described in subclause 4.5.5.0.

Upon deactivation or removal of a PCC rule, the PCEF shall free the resources reserved for that PCC rule.

4.5.5.4 Coordination of authorized QoS scopes in mixed mode

Coordination of authorized QoS scopes in mixed mode is access specific. See Annex A for further details.

4.5.5.5 Provisioning of authorized QoS per QCI

The PCRF may provision an authorized QoS per QCI for non-GBR bearer QCI values. The PCRF shall not provision an authorized QoS per QCI for GBR bearer QCI values.

The authorized QoS per QCI shall be provisioned at RAR or CCA command level using the QoS-Information AVP with the QoS-Class-Identifier AVP and the Maximum-Requested-Bandwidth-UL AVP and/or the Maximum-Requested-Bandwidth-DL AVP. The Guaranteed Bitrate values shall not be filled up. Multiple QoS-Information AVPs can be used for assigning authorized QoS for several QCIs with one command. The authorized QoS per QCI may be provisioned before or in connection with the activation of the first PCC rule with a certain QCI. The PCRF may also provision a changed authorized QoS per QCI at any time.

4.5.5.6 Policy enforcement for authorized QoS per QCI

The PCEF can receive an authorized QoS per QCI for non GBR-bearer QCI values. It sets an upper limit for the MBR that the PCEF may assign to a non-GBR bearer with that QCI. If the PCEF receives an authorized QoS per QCI for a non-GBR bearer QCI value, it shall not set a higher MBR for that bearer than the provisioned MBR.The PCEF should assign the authorized MBR per QCI to a non-GBR bearer with that QCI to avoid frequent IP-CAN bearer modifications as PCC rules can be dynamically activated and deactivated.

If multiple IP-CAN bearers within the same IP-CAN session are assigned the same QCI, the authorized MBR per QCI applies independently to each of those IP-CAN bearers.

The access-specific BS Manager (as included in [8]) within the PCEF receives the authorized access-specific QoS information from the Translation/mapping function.

4.5.5.7 Provisioning of authorized QoS per APN

Provisioning of authorized QoS per APN is 3GPP-EPS access specific. See Annex B for further information.

4.5.5.8 Policy enforcement for authorized QoS per APN

Policy enforcement for authorized QoS per QCI is 3GPP-EPS access specific. See Annex B for further information.

4.5.5.9 Provisioning of authorized QoS for the Default EPS Bearer

The PCRF may provision the authorized QoS for the default EPS bearer. The authorized QoS may be obtained upon interaction with the SPR.

The default EPS bearer QoS information shall be provisioned at RAR or CCA command level using the Default-EPS-Bearer-QoS AVP including the QoS-Class-Identifier AVP and the Allocation-Retention-Priority AVP. The provided QoS-Class-Identifier AVP shall include a non-GBR corresponding value.

4.5.5.10 Policy enforcement for authorized QoS of the Default EPS Bearer

The PCEF may receive the authorized QoS for the default bearer over Gx interface. The PCEF enforces it which may lead to the upgrade or downgrade of the subscribed default EPS Bearer QoS.

4.5.6 Indication of IP-CAN Bearer Termination Implications

This procedure applies to those IP-CAN networks that support multiple bearers. This procedure applies only to dedicated bearers. For 3GPP-GPRS IP-CAN network, see annex A.

If the last IP CAN bearer within an IP CAN session is being terminated, the PCEF shall apply the procedures in clause 4.5.7 to indicate the IP CAN session termination.

The PCEF shall inform the PCRF whenever one of these conditions applies.

- There is a bearer resource modification request initiated by the UE that requires the release of resources
- The PCEF is requested to initiate the deactivation of a bearer
- PCC rule(s) are disabled
- Based on the response from the PCRF, the PCEF may initiate the termination of the bearer.

Editor's Note: It is ffs if the indication of bearer termination is also applicable if the provisioned total QoS is reduced compared to what has been provisioned in the Authorized-QoS AVP on session level.

The "Indication of IP-CAN Bearer Termination Implications" procedure shall be carried out as part of a Request for PCC rules at IP-CAN session modification. The PCEF shall send a CC-Request with CC-Request-Type AVP set to the value "UPDATE_REQUEST" and shall include the following additional information:

- The PCEF shall include the Charging-Rule-Report AVP with the PCC-Rule-Status set to inactive for the affected PCC rules.

When the PCRF receives the CC-Request indicating the implications of a bearer termination, it shall acknowledge the message by sending a CC-Answer to the PCEF. The PCRF has the option to make a new PCC decision for the affected PCC Rules. Within the CC-answer, the PCRF may request the removal of the affected PCC rules and provision PCC rules as detailed in clause 4.5.2.

The PCEF shall remove all PCC rules which have not been re-installed.

If no more PCC rules are active as part of the bearer, the PCEF shall initiate the IP-CAN bearer termination procedure.

The PCRF is not aware that it requests the termination of an IP CAN bearer by removing certain PCC rules. If upon removal of the PCC rules, there are no more PCC rules active in the PCEF for an IP-CAN bearer, the PCEF shall initiate the bearer termination procedure.

Signalling flows for the IP-CAN bearer termination and details of the binding mechanism are presented in 3GPP TS 29.213 [8].

4.5.7 Indication of IP-CAN Session Termination

The PCEF shall contact the PCRF when the IP-CAN session is being terminated. The PCEF shall send a CC-Request with CC-Request-Type AVP set to the value "TERMINATION_REQUEST".

When the PCRF receives the CC-Request, it shall acknowledge this message by sending a CC-Answer to the PCEF.

NOTE: According to DCC procedures, the Diameter Credit Control session is being terminated with this message exchange.

Signalling flows for the IP-CAN session termination are presented in 3GPP TS 29.213 [8].

4.5.8 Request of IP-CAN Bearer Termination

This procedure applies to those IP-CAN networks that support multiple bearers. This procedure applies only to dedicated bearers. For 3GPP-GPRS IP-CAN network, see annex A.

As a consequence of the removal of PCC rules initiated by the PCRF, the PCEF may require the termination of an existing bearer. The PCRF may not be aware that it requests the termination of an IP-CAN bearer by removing certain PCC rules.

The PCRF may request the removal of the PCC rules by using the PCC rule provisioning procedures in clause 4.5.2 to remove all PCRF-provisioned PCC rules and deactivate all PCC rules predefined within the PCEF.,The PCRF may either completely remove these PCC rules from the IP CAN session or reinstall them (e.g. by changing the QoS or charging information) within the IP CAN session. When all the PCC rules applied to one bearer have been deleted and/or deactivated, the PCEF will instantly start the bearer termination procedure.

If the selected Bearer Control Mode (BCM) is UE-only, and the PCRF receives a trigger for the removal of all PCC rules from the AF, the following steps apply. In order to avoid race conditions, the PCRF should start a timer to wait for the UE-initiated resource release message. If a UE-initiated resource release is performed before timer expiry, the PCRF will receive an Indication of IP-CAN Bearer Termination Implications according to Clause 4.5.6 and shall then not perform the removal of the PCC rules. Otherwise, if the timer expires, the PCRF shall remove/deactivate the affected PCC rules that have been previously installed/activated..

If the selected BCM is UE-only, and the PCRF decides to remove one or more PCC rules due to an internal trigger or trigger from the SPR, the PCRF shall instantly remove/deactivate the affected PCC rules that have been previously installed/activated..

If the selected BCM is UE/NW, and the PCRF removes/deactivates at the PCEF, all PCC rules bound to an IP CAN bearer (due to any trigger), the PCEF shall instantly start the procedures to terminate the related IP-CAN bearer.

If no more PCC rules are applied to an IP CAN bearer, the PCEF shall apply IP CAN specific procedures to terminate the IP CAN bearer, if such procedures exist for this IP CAN type. Furthermore, the PCEF shall apply the indication of IP CAN Bearer Termination procedure in clause 4.5.6.

4.5.9 Request of IP-CAN Session Termination

If the PCRF decides to terminate an IP CAN session due to an internal trigger or trigger from the SPR, the PCRF shall send an RAR command including the Session-Release-Cause AVP to the PCEF. The PCEF shall acknowledge the command by sending an RAA command to the PCRF and instantly remove/deactivate all the PCC rules that have been previously installed or activated on that IP-CAN session.

The PCEF shall apply IP CAN specific procedures to terminate the IP CAN session. Furthermore, the PCEF shall apply the indication of IP CAN Session Termination procedure in clause 4.5.7.

See Annex A for 3GPP-GPRS access type.

4.5.10 Bearer Control Mode Selection

The PCEF may indicate, via the Gx reference point, a request for Bearer Control Mode (BCM) selection at IP-CAN session establishment or IP-CAN session modification (e.g. as a consequence of an SGSN change). It will be done using the PCC rule request procedure.

At IP-CAN Session Establishment, the PCEF will supply, if available, the Network-Request-Support AVP in the CC-Request with a CC-Request-Type AVP set to the value 'INITIAL_REQUEST'. The Network-Request-Support AVP indicates the access network support of the network requested bearer control.

The PCRF derives the selected Bearer-Control-Mode AVP based on the received Network-Request-Support AVP, access network information, subscriber information and operator policy. If the selected bearer control mode is UE_NW, the PCRF shall decide what mode (UE or NW) shall apply for every PCC rule.

NOTE: For operator-controlled services, the UE and the PCRF may be provisioned with information indicating which mode is to be used.

The selected Bearer-Control-Mode AVP shall be provided to the PCEF using the PCC Rules provision procedure at IP-CAN session establishment. The selected value will be applicable for the whole IP-CAN session.

NOTE: This scenario will likely happen when there is PLMN change that force a BCM change to UE-only due to the lack of support of network initiated procedures. There are several valid solutions such as enforcing the IP-CAN termination, or retaining the IP-CAN session with either all the bearers or only with the bearers with bearer binding related to UE-only procedures. A preferred solution is not specified in Rel-8 and is left as an implementation choice.

Editor"s Note: It is ffs if the note above applies for scenarios like BBERF relocation or multiple BBERF support within an IP-CAN session where the BCM may change between UE_ONLY and UE_NW.

4.5.11 Provisioning of Event Report Indication

For the cases where Gxa and/or Gxc are deployed in the network, the PCEF may indicate the PCRF to be informed about specific changes occurred in the access network. In this case, the PCRF shall subscribe to the appropriate event triggers in the BBERF according to clause 4a.5.8. The Event Report concept is defined in 3GPP TS 23.203 [7] clause 3.1.

When PCRF is notified that an event is triggered in the BBERF, if the PCEF has previously requested to be informed of the specific event, the PCRF shall notify the PCEF about the event occurred together with additional related information. This notification will be done by using the Event-Report-Indication AVP. There may be neither PCC Rules nor Event Triggers in this message.

4.5.12 PCC Rule Error Handling

If the installation/activation of one or more PCC rules fails, the PCEF shall include one or more Charging-Rule-Report AVP(s) in either a CCR or an RAA command as described below for the affected PCC rules. Within each Charging-Rule-Report AVP, the PCEF shall identify the failed PCC rule(s) by including the Charging-Rule-Name AVP(s) or Charging-Rule-Base-Name AVP(s), shall identify the failed reason code by including a Rule-Failure-Code AVP, and shall include the PCC-Rule-Status AVP as described below:

- If the installation/activation of one or more PCC rules fails using a PUSH mode (i.e., the PCRF installs/activates a rule using RAR command), the PCEF shall communicate the failure to the PCRF in the RAA response to the RAR.

- If the installation/activation of one or more PCC rules fails using a PULL mode (i.e., the PCRF installs/activates a rule using a CCA command) the PCEF shall send the PCRF a new CCR command and include the Rule-Failure-Code AVP.

If the installation/activation of one or more new PCC rules (i.e., rules which were not previously successfully installed) fails, the PCEF shall set the PCC-Rule-Status to INACTIVE for both the PUSH and the PULL modes.

Editor's Note: If a PCC rule modification fails (i.e., the PCRF installs a PCC rule which was previously successfully installed) it is FFS whether the PCEF may set the PCC-Rule-Status to ACTIVE or INACTIVE.

If a PCC rule was successfully installed/activated, but can no longer be enforced by the PCEF, the PCEF shall send the PCRF a new CCR command and include a Charging-Rule-Report AVP. The PCEF shall include the Rule-Failure-Code AVP within the Charging-Rule-Report AVP and shall set the PCC-Rule-Status to INACTIVE.

NOTE: The status of the rule must be INACTIVE when reporting an error in a new CCR command since the new CCR/CCA transaction contains no previous state information regarding the definition and status of the rule.

4.5.13 Time of the day procedures

PCEF shall be able to perform PCC rule request as instructed by the PCRF. Revalidation-Time when set by the PCRF, shall cause the PCEF to trigger a PCRF interaction to request PCC rules from the PCRF for an established IP CAN session. The PCEF shall stop the timer once the PCEF triggers an REVALIDATION_TIMEOUT event.

PCRF shall be able to provide a new value for the revalidation timeout by including Revalidation-Time in CCA or RAR

PCRF shall be able to stop the revalidation timer by disabling the REVALIDATION_TIMEOUT event trigger.

If Rule-Activation-Time is specified, then the PCEF shall set the rule active after that time.

If Rule-Deactivation-Time is specified, then the PCEF shall set the rule to be inactive after that time.

PCC Rule Activation or Deactivation will not generate any CCR commands with Charging-Rule-Report since PCRF is already aware of the state of the rules.

If Rule-Activation-Time or Rule-Deactivation-Time is specified in the Charging-Rule-Install then it will replace the previously set values for the specified PCC rules.

The PCC rule shall be inactive when the rule is installed.

The 3GPP-MS-TimeZone AVP, if available, may be used for the PCRF to derive the Rule-Activation-Time and Rule-Deactivation-Time.

Editor's Note: The 3GPP-MS-TimeZone AVP, if available, will be sent to the PCRF during the IP-CAN session establishment. If the UE moves to another time zone, it is FFS how the PCEF reports the updated UE time zone information to the PCRF. It is FFS if the UE time zone information is needed over Gxx from the BBERF.

Editor's Note: BBERF interaction for time of the day updates is TBD.

4a Gxx reference points

Editor's note: The structure of this clause may change

4a.1 Overview

The Gxx reference point is located between the Policy and Charging Rules Function (PCRF) and the Bearer Binding and Event Reporting Function (BBERF). Gxc applies when the BBERF is located in the S-GW and Gxa applies when the BBERF is located in a trusted non-3GPP access. The Gxx reference point is used for:

- Provisioning, update and removal of QoS rules from the PCRF to the BBERF
- Transmission of traffic plane events from the BBERF to the PCRF.
- Transmission of events reported by the PCEF to the BBERF via the PCRF.

The stage 2 level requirements for the Gxx reference point are defined in 3GPP TS 23.203 [7] and 3GPP TS 23.402 [23].

Signalling flows related to Rx, Gx and Gxx interfaces are specified in 3GPP TS 29.213 [8].

4a.2 Gxx Reference model

The Gxx reference point is defined between the PCRF and the BBERF. The BBERF is located in the AN-Gateway. The AN-Gateway is the S-GW when Gxc applies and it is the trusted non-3GPP access gateway when Gxa applies. The relationships between the different functional entities involved are depicted in figure 4a.2.1

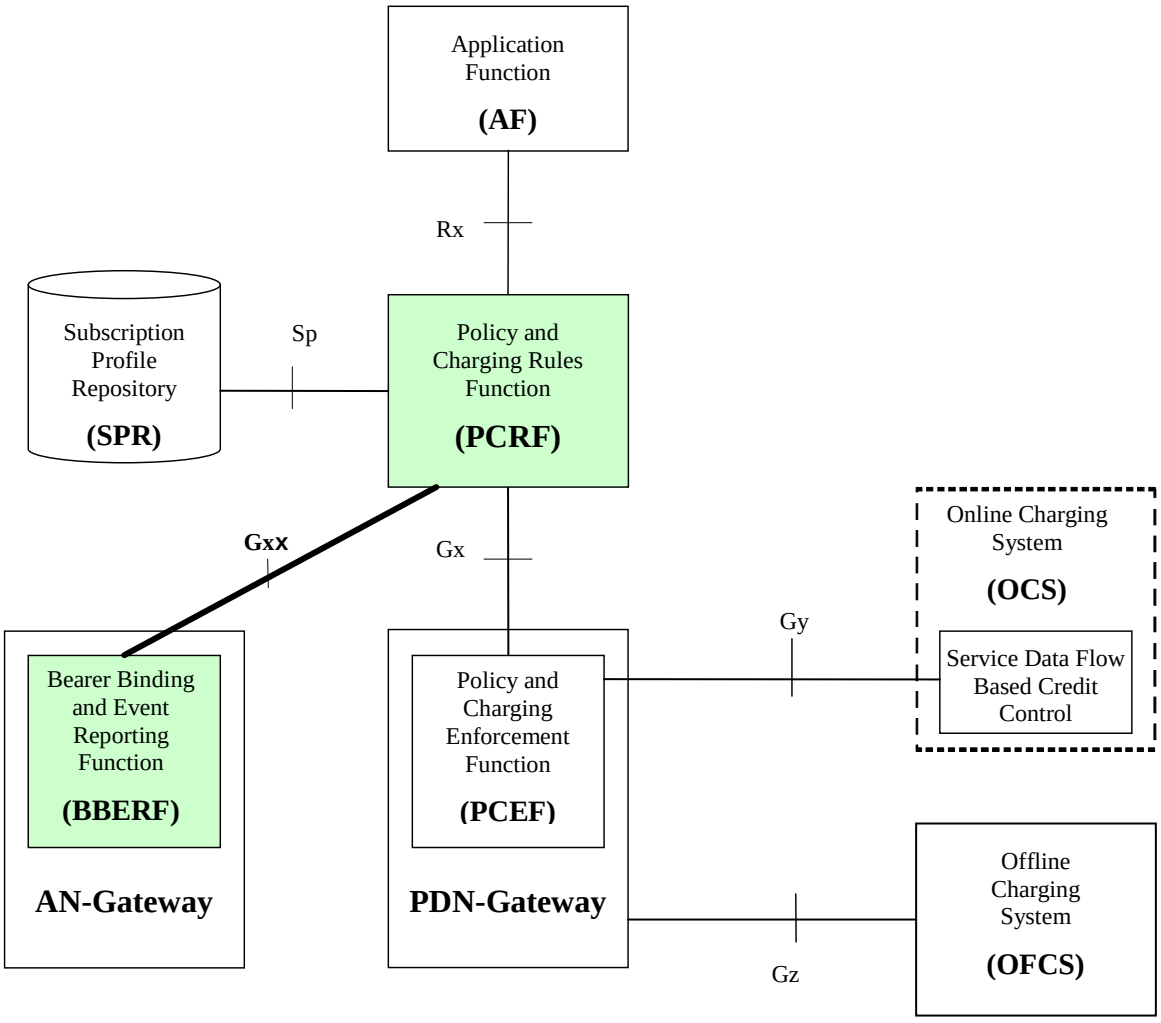

Figure 4a.2.1: Gxx reference point at the Policy and Charging Control (PCC) architecture

NOTE: The details associated with the Sp reference point are not specified in this Release. The SPR"s relation to existing subscriber databases is not specified in this Release.

4a.3 Quality of Service Control Rules

4a.3.1 Quality of Service Control Rule Definition

The purpose of the Quality of Service Control rule (QoS rule) for the BBERF is to:

- Detect a packet belonging to a service data flow.
  - The service data flow filters within the QoS rule are used for the selection of downlink IP CAN bearers.

  - The service data flow filters within the QoS rule are used for the enforcement that uplink IP flows are transported in the correct IP CAN bearer.

- Identify the service the service data flow contributes to.

The QoS rules are derived from the PCC rules. The same service data flow template, precedence and the QoS information of a QoS rule shall also be defined in a corresponding PCC rule.

The BBERF shall select a QoS rule for each received packet by evaluating received packets against service data flow filters of QoS rules in the order of the precedence of the QoS rules. When a packet matches a service data flow filter, the packet matching process for that packet is completed, and the QoS rule for that filter shall be applied.

A QoS rule consists of:

- a rule name;
- service data flow filter(s);
- precedence;
- QoS parameters;

The rule name shall be used to reference a QoS rule in the communication between the BBERF and the PCRF.

The service flow filter(s) shall be used to select the traffic for which the rule applies.

The QoS information includes the QoS class identifier (authorized QoS class for the service data flow), the ARP and authorized bitrates for uplink and downlink.

For different QoS rules with overlapping service data flow filter, the precedence of the rule determines which of these rules is applicable.

4a.3.2 Operations on QoS Rules

The following operations are available:

- Installation: to provision a QoS rule that has not been already provisioned.
- Modification: to modify a QoS rule already installed.
- Removal: to remove a QoS rule already installed.

The procedures to perform these operations are further described in clause 4a.5.2.

4a.4 Functional elements

4a.4.1 PCRF

The PCRF has been already specified in clause 4.4.1. Particularities for the Gxx reference point are specified in this clause.

The PCRF shall provision QoS Rules to the BBERF via the Gxx reference point.

The PCRF shall provide QoS rules with identical service data flow templates as provided to the PCEF in the PCC rules. If the service data flow is tunnelled at the BBERF, the PCRF shall provide the BBERF with mobility protocol tunnelling header information received from the PCEF to enable the service data flow detection in the mobility tunnel at the BBERF

The PCRF QoS Rule decisions may be based on one or more of the following:

- Information obtained from the AF via the Rx reference point, e.g. the session, media and subscriber related information.

- Information obtained from the PCEF via the Gx reference point, e.g. IP-CAN bearer attributes, request type and subscriber related information.
- Information obtained from the SPR via the Sp reference point, e.g. subscriber and service related data.
- Information obtained from the BBERF via the Gxx reference point.

The PCRF shall inform the BBERF through the use of QoS rules on the treatment of each service data flow that is under PCC control, in accordance with the PCRF policy decision(s).

Upon subscription to loss of AF signalling bearer notifications by the AF, the PCRF shall request to BBERF to be notified of the loss of resources associated to the QoS Rules corresponding with AF Signalling IP Flows, if this has not been requested previously to the BBERF. In this case, PCRF will not subscribe to this event in the PCEF.

The PCRF shall, based on information reported from BBERF and PCEF, determine the Gx session(s) that shall be linked with a Gateway Control session.

4a.4.2 BBERF

The BBERF (Bearer Binding and Event Reporting Function) is a functional element located in the S-GW when Gxc applies and in a trusted non-3GPP access when Gxa applies. It provides control over the user plane traffic handling and encompasses the following functionalities:

- Bearer binding: For a service data flow that is under QoS control, the Bearer Binding Function (BBF) within BBERF shall ensure that the service data flow is carried over the bearer with the appropriate QoS class.
- Uplink bearer binding verification.
- Event reporting: The BBERF shall report events to the PCRF based on the event triggers installed by the PCRF.
- Service data flow detection for tunnelled and untunelled SDFs: The BBERF uses service data flow filters received from the PCRF for service data flow detection.
- Service data flow detection for tunnelled SDFs: For the selection of the service data flow filters to apply the BBERF shall use a match with the tunnelling associated tunnelling header information received from the PCRF as a prerequisite.

If requested by the PCRF, the BBERF shall report to the PCRF when the status of the related service data flow changes.

4a.5 PCC procedures over Gxx reference points

4a.5.1 Gateway control and QoS Rules Request

The BBERF shall indicate, via the Gxx reference point, a request for QoS rules in the following instances:

1) At Gateway Control Session Establishment:

The BBERF shall send a CCR command with the CC-Request-Type AVP set to the value "INITIAL_REQUEST". The CCR command shall include the IMSI within the Subscription-Id AVP. If available, the BBERF shall supply additional parameters to allow the PCRF to identify the rules to be applied : the type of IP-CAN within the IP-CAN-Type AVP, the type of the radio access technology within the RAT-Type AVP, the PDN information , the PLMN id, the UE IP address (es), information about the user equipment within User-Equipment-Info AVP, QoS information within QoS-Information-AVP, user location information, the access network gateway address and an indication if the default bearer is used for IMS. Furthermore, if the UE and the network support the network-initiated procedures, the BBERF shall indicate this by supplying the Network-Request-Support AVP.

For IP-CAN types that support multiple IP-CAN bearers, the BBERF may provide the Default-EPS-Bearer-QoS AVP including the ARP and QCI values corresponding to the Default EPS Bearer QoS.

Editor"s note: It"s ffs to assign a proper AVP to some of the parameters listed above.

2) At Gateway Control Session Modification:

The BBERF shall send a CC-Request with CC-Request-Type AVP set to the value "UPDATE_REQUEST". For a Gateway Control and QoS Rules request where an existing IP-CAN resource is modified, the BBERF shall supply within the QoS rule request the specific event which caused such request (within the Event-Trigger AVP) and any previously provisioned QoS rule(s) affected by the gateway control and QoS Rules request. The affected QoS Rules and their status shall be supplied to the PCRF within the QoS-Rule-Report AVP.

QoS rules can also be requested as a consequence of a failure in the QoS rule installation or enforcement without requiring an Event-Trigger. See clause 4a.5.4.

If the PCRF is, due to incomplete, erroneous or missing information (e.g. subscription related information not available or authorized QoS exceeding the subscribed bandwidth) not able to provision a policy decision as response to the request for QoS Rules by the BBERF, the PCRF may reject the request using a CC Answer with the Gx experimental result code DIAMETER_ERROR_INITIAL_PARAMETERS (5140). If the BBERF receives a CC Answer with this code, the BBERF shall reject the gateway control and QoS Rules request.

4a.5.2 Gateway control and QoS Rules Provision

The PCRF may decide to operate on QoS Rules without obtaining a request from the BBERF, e.g. in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF, or from a trigger by the SPR. To operate on QoS Rules without a request from the BBERF, the PCRF shall include these QoS Rules in an RA-Request message within either the QoS-Rule-Install AVP or the QoS-Rule-Remove AVP.

The BBERF shall reply with an RA-Answer. If the corresponding IP-CAN resource cannot be established or modified to satisfy the bearer binding, then the BBERF shall reject the activation of a QoS rule using the Gxx experimental result code DIAMETER_BEARER_EVENT and a proper Event-Trigger value. Depending on the cause, the PCRF can decide if re-installation, modification, removal of QoS Rules or any other action apply.

The PCRF shall indicate, via the Gxx reference point, QoS rules to be applied at the BBERF. This may be using one of the following procedures:

- PULL procedure(Provisioning solicited by the BBERF): In response to a request for QoS rules being made by the BBERF, as described in the preceding section, the PCRF shall provision QoS rules in the CC-Answer; or

- PUSH procedure(Unsolicited provisioning): The PCRF may decide to provision QoS rules without obtaining a request from the BBERF, e.g. in response to information provided to the PCRF via the Rx reference point, or in response to an internal trigger within the PCRF. To provision QoS rules without a request from the BBERF, the PCRF shall include these QoS rules in an RA-Request message.

For each request from the BBERF or upon the unsolicited provision the PCRF shall provision zero or more QoS rules. The PCRF may perform an operation on a single QoS rule by one of the following means:

- To install or modify a PCRF-provisioned QoS rule, the PCRF shall provision a corresponding QoS-Rule-Definition AVP within a QoS-Rule-Install AVP.

- To remove a QoS rule which has previously been provisioned by the PCRF, the PCRF shall provision the name of this rule as value of a QoS-Rule-Name AVP within a QoS-Rule-Remove AVP.

The PCRF may combine multiple of the above QoS rule operations in a single CC-Answer command or RA-Request command..

To install a new or modify an already installed PCRF defined QoS rule, the QoS-Rule-Definition AVP shall be used. If a QoS rule with the same rule name, as supplied in the QoS-Rule-Name AVP within the QoS-Rule-Definition AVP, already exists at the BBERF, the new QoS rule shall update the currently installed rule. If the existing QoS rule already has attributes also included in the new QoS rule definition, the existing attributes shall be overwritten. Any attribute in the existing QoS rule not included in the new QoS rule definition shall remain valid.

If the provisioning of QoS rules fails, the BBERF informs the PCRF as described in Clause 4a.5.4 QoS Rule Error Handling. If the corresponding IP-CAN bearer can not be established or modified, then the BBERF shall reject the activation of a QoS rule using the Gxx experimental result code DIAMETER_BEARER_EVENT and a proper Rule Failure Code. Depending on the cause, PCRF can decide if re-installation, modification, removal of QoS rules or any other action apply.

If the PCRF is unable to create a QoS rule for the response to the CC Request by the PCEF, the PCRF may reject the request as described in subclause 4a5.1.

4a.5.3 Gateway Control Session Termination

The BBERF shall contact the PCRF when the gateway control session is being terminated (e.g. detach). The BBERF shall send a CC-Request with CC-Request-Type AVP set to the value "TERMINATION_REQUEST".

When the PCRF receives the CC-Request, it shall acknowledge this message by sending a CC-Answer to the BBERF.

4a.5.4 Request of Gateway Control Session Termination

The PCRF may request the termination of a gateway control session.

If the PCRF decides to terminate a gateway control session due to an internal trigger or trigger from the SPR, the PCRF shall send an RAR command including the Session-Release-Cause AVP to the BBERF. When the BBERF receives the RAR Command, it shall acknowledge the command by sending an RAA command to the PCRF and instantly remove all the QoS rules that have been previously installed on that gateway control session. And then the BBERF shall apply the gateway control session termination procedure in Clause 4a.5.3.

4a.5.5 QoS Control Rule error handling

The same error handling behaviour as defined in clause 4.5.12 shall apply for QoS control rules,. However, QoS-Rule-Report AVP shall be used to report the affected QoS rules instead of Charging-Rule-Report AVP.

4a.5.6 Gateway Control session to Gx session linking

For the cases where Gxx is deployed in the network, the PCRF shall determine at IP-CAN session establishment, which open Gateway Control session applies to the new established IP-CAN session.

If the already established Gateway Control session for that subscriber is not related with a PDN identifier (i.e. the Called-Station-Id AVP was not received at Gateway Control Session Establishment), the PCRF shall determine that the IP-CAN session being established corresponds to that Gateway Control Session if the following conditions are fulfilled:

- The CoA-IP-Address AVP received in the IP-CAN session establishment matches the Framed-IP-Address or Framed-IPv6-Prefix received during the Gateway Control Session Establishment and

- The Subscription-Id AVP received in the IP-CAN session establishment matches the Subscription-Id AVP received during the Gateway Control Session Establishment

In this case, the PCRF may have more than one IP-CAN Gx session linked to the Gateway Control session.

If the already established Gateway Control session for that subscriber is related with a PDN identifier (i.e. the Called-Station-Id AVP was received during the Gateway Control Session Establishment), the PCRF shall determine that the IP-CAN session being established corresponds to that Gateway Control Session if the following conditions are fulfilled:

- The Called-Station-Id AVP received in the IP-CAN session establishment matches the Called-Station-Id AVP received during the Gateway Control Session Establishment and

- The Subscription-Id AVP received in the IP-CAN session establishment matches the Subscription-Id AVP received during the Gateway Control Session Establishment

In this case, the PCRF shall have only one IP-CAN Gx session linked to the Gateway Control session.

For the cases of BBERF relocation and BBERF pre-registration, upon reception of a Gateway Control Session Establishment, the PCRF shall be able to determine the Gx session(s) that apply to the new established Gateway Control session as follows:

- If the new Gateway Control session for that subscriber is not related with a PDN identifier (i.e. the Called-Station-Id AVP was not received at Gateway Control Session Establishment), the PCRF shall determine the Gx session(s) that correspond to that Gateway Control Session if the following conditions are fulfilled:

- The Framed-IP-Address or Framed-IPv6-Prefix received in the Gateway Control Session Establishment matches the CoA-IP-Address AVP for the IP-CAN session(s) and

- If received, the Subscription-Id AVP received in the Gateway Control Session Establishment matches the Subscription-Id for the IP-CAN sessions(s)

- If the new Gateway Control session for that subscriber is related with a PDN identifier (i.e. the Called-Station-Id AVP is received) the PCRF shall determine the Gx session that correspond to the Gateway Control Session if at least two of the following conditions are fulfilled:

  - The Called-Station-Id AVP is received in the Gateway Control Session Establishment and it matches the APN of the Gx session and

  - The Subscription-Id AVP received in the Gateway Control Session Establishment matches the Subscription-Id for the IP-CAN session(s) and

  - If received, the Framed-IP-Address AVP or Framed-IPv6-Prefix AVP included in the Gateway Control Session Establishment matches the Framed-IP-Address AVP or Framed-IPv6-Prefix AVP of the Gx session

In this case, the PCRF shall link the Gateway Control Session to the Gx session.

4a.5.7 Multiple BBERF support

This procedure takes place during the handover situations where one or more BBERF can establish a Gateway Control Session as part of a pre-registration procedure.

The PCRF, based on information received from the BBERF and PCEF, shall identify the BBERF as primary or non-primary.

Upon receiving a Gateway Control Session Establishment request from a new BBERF and if the PCRF identifies multiple Gateway Control sessions involved for a particular IP-CAN session (i.e. multiple BBERF connections during handovers) the PCRF shall carry out the following procedures:

- The PCRF shall identify the Gateway Control session that reported the same IP-CAN type as reported by PCEF and classify the BBERF that initiated that Gateway Control session as 'primary'.

- In the case where more that one Gateway Control sessions reported the same IP-CAN type as reported by PCEF the PCRF shall classify the BBERF that initiated the last Gateway Control session as 'primary'

- The remaining BBERF connections shall be classified by the PCRF as 'non-primary'

Upon reception of a CCR command over the Gx interface indicating 'UPDATE_REQUEST' (i.e. as part of the an IP-CAN session modification procedure), the PCRF shall carry out the above classification procedures again for primary/non-primary BBERFs if the IP-CAN type changes as part of the IP-CAN session modification procedure.

During the Gateway Control and QoS Rule Request, the PCRF shall act as follows with regards to the Gxx reference point:

- In the response to a CCR command with the CC-Request-Type AVP set to the value "INITIAL_REQUEST", if the BCM selected by the PCRF for that BBERF (primary/non-primary) indicates UE_NW, the PCRF shall provision the applicable active QoS rules for the linked IP-CAN session in the QoS-Rule-Install AVP in the CC-Answer command. In the case of non-primary BBERF, only those that do not require any modification for the active PCC rules will be provided.

- In the response of a CCR command with the CC-Request-Type set to the value 'INITIAL_REQUEST', if the BCM selected by the PCRF for that BBERF (primary/non-primary) that initiated the Gateway Control session indicates UE_ONLY, the PCRF shall only include QoS rules applicable to the default bearer in the CC-Answer command.

- In the response to a CCR command with the CC-Request-Type set to the value 'UPDATE_REQUEST' initiated by a BBERF that the PCRF has classified as non-primary, including an Event-Trigger AVP indicating bearer resource modification request, the PCRF shall create the QoS rules based on the traffic mapping information received in the request and check whether there are aligned PCC rules installed in the PCEF. If the aligned PCC rules active in the PCEF require no modification, the PCRF shall provision the QoS rules within the QoS-Rule-

Install AVP to the non-primary BBERF that created the request. Otherwise, the PCRF shall reject the request using the Gxx experimental result code DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED.

Editor"s Note: Bearer Resource Modification event trigger value is TBD.

- In the response to a CCR command with the CC-Request-Type set to the value 'UPDATE_REQUEST' initiated by a BBERF including any other event trigger within the Event-Trigger AVP, the PCRF shall provision/modify/remove the applicable QoS rules in the CC-Answer command when the BBERF is selected as primary. Otherwise, only QoS rules with aligned active PCC rules will be provided.

NOTE: The PCRF shall only operate on the PCC rules towards the PCEF when the CCR command was received from a primary BBERF.

For unsolicited provisioning of QoS rules, the PCRF shall provision the applicable QoS rules (those that are Nw-init) to those BBERFs where the Bearer Control Mode is UE_NW.

For the case where the primary BBERF rejects the installation of one or more QoS rule(s) in a RA-Answer command, the PCRF shall remove the impacted QoS rules from all the non-primary BBERFs in a RAR message including the removed QoS rules in the QoS-Rule-Remove AVP. If a non-primary BBERF rejects the installation of one or more QoS rules the PCRF shall not take any action towards the PCEF and BBERFs regarding the rejected rules.

If a primary BBERF reported the failure in a new CC-Request command, the PCRF shall remove the impacted QoS rules in the CC-Answer command and shall initiate a RA-Request command towards all the non-primary BBERFs including the removed QoS rules in the QoS-Rule-Remove AVP. If the BBERF that reported the failure is a non-primary BBERF, the PCRF shall acknowledge the Diameter CCR with a CCA command and shall not take further action towards the PCEF and BBERFs regarding the failed rules.

When the PCEF subscribes to events by using the Event-Report-Indication AVP, the PCRF shall provision those events only in the primary BBERF.

4a.5.8 Provisioning of Event Triggers

The PCRF may provide one or several event triggers within one or several Event-Trigger AVP to the BBERF using the Gateway Control and QoS rule provision procedure. Event triggers may be used to determine which specific event causes the BBERF to re-request QoS rules. Provisioning of event triggers will be done at Gateway Control session level. The Event-Trigger AVP may be provided either in combination with the initial or subsequent QoS rule provisioning.

The PCEF may request the PCRF to be informed about specific changes occurred in the access network as indicated in clause 4.5.11. In this case, the PCRF shall additionally subscribe to the corresponding event triggers at the BBERF.

The PCRF may add new event triggers or remove the already provided ones at each request from the BBERF or upon the unsolicited provision from the PCRF. In order to do so, the PCRF shall provide the new complete list of applicable event triggers related to the Gateway Control session including the needed provisioned Event-Trigger AVPs in the CCA or RAR commands.

The PCRF may remove all previously provided event triggers by providing the Event-Trigger AVP set to the value NO_EVENT_TRIGGERS. When an Event-Trigger AVP is provided with this value, no other Event-Trigger AVP shall be provided in the CCA or RAR command. Upon reception of an Event-Trigger AVP with this value, the BBERF shall not inform PCRF of any event that requires to be provisioned from the PCRF.

If no Event-Trigger AVP is included in a CCA or RAR operation, any previously provisioned event trigger will be still applicable.

4a.5.9 Bearer Control Mode Selection

The BBERF may indicate, via the Gxx reference point, a request for Bearer Control Mode (BCM) selection at Gateway Control session establishment or Gateway Control Session modification (e.g. as a consequence of an SGSN change). It will be done using the Gateway Control and QoS rule request procedure.

The BBERF will supply, if available, the Network-Request-Support AVP in the CC-Request with a CC-Request-Type AVP set to the value 'INITIAL_REQUEST'. The Network-Request-Support AVP indicates the access network support of the network requested bearer control.

The PCRF derives the selected Bearer-Control-Mode AVP based on the received Network-Request-Support AVP, access network information, subscriber information and operator policy. If the selected bearer control mode is UE_NW, the PCRF shall decide what mode (UE or NW) shall apply for every QoS rule.

NOTE: For operator-controlled services, the UE and the PCRF may be provisioned with information indicating which mode is to be used.

The selected Bearer-Control-Mode AVP shall be provided to the BBERF using the Gateway Control and QoS Rules provision procedure at Gateway Control session establishment. The selected value will be applicable for the whole Gateway Control session.

Editor"s Note: It is ffs the different scenarios where the BCM changes between UE_ONLY and UE_NW.

5 Gx protocol

5.1 Protocol support

The Gx protocol in the present release is based on Gx protocol defined for Release 6 as specified in 3GPP TS 29.210 [2]. However, due to a new paradigm (DCC session for an IP-CAN session) between Release 6 and the present release, the Gx application in the present release has an own vendor specific Diameter application.

The Gx application is defined as a vendor specific Diameter application, where the vendor is 3GPP and the Application-ID for the Gx Application in the present release is 16777238. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

NOTE: A route entry can have a different destination based on the application identification AVP of the message. Therefore, Diameter agents (relay, proxy, redirection, translation agents) must be configured appropriately to identify the 3GPP Gx application within the Auth-Application-Id AVP in order to create suitable routeing tables.

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

With regard to the Diameter protocol defined over the Gx interface, the PCRF acts as a Diameter server, in the sense that it is the network element that handles PCC Rule requests for a particular realm. The PCEF acts as the Diameter client, in the sense that is the network element requesting PCC rules in the transport plane network resources.

5.2 Initialization, maintenance and termination of connection and session

The initialization and maintenance of the connection between each PCRF and PCEF pair is defined by the underlying protocol. Establishment and maintenance of connections between Diameter nodes is described in RFC 3588 [5].

After establishing the transport connection, the PCRF and the PCEF shall advertise the support of the Gx specific Application by including the value of the application identifier in the Auth-Application-Id AVP and the value of the 3GPP (10415) in the Vendor-Id AVP of the Vendor-Specific-Application-Id AVP contained in the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in the Diameter Base Protocol (RFC 3588 [5]).

The termination of the Diameter user session is specified in RFC 3588 [5] in clauses 8.4 and 8.5. The description of how to use of these termination procedures in the normal cases is embedded in the procedures description.

5.3 Gx specific AVPs

Table 5.3.1 describes the Diameter AVPs defined for the Gx reference point, their AVP Code values, types, possible flag values, whether or not the AVP may be encrypted, what access types (e.g. 3GPP-GPRS, etc.) the AVP is applicable

to and the applicability of the AVPs to charging control, policy control or both. The Vendor-Id header of all AVPs defined in the present document shall be set to 3GPP (10415).

Table 5.3.1: Gx specific Diameter AVPs

Attribute Name	AVP Code	Clause defined	Value Type (note 2)	AVP Flag rules (note 1)				May Encr.	Acc. type	Applicability (note 3)
				Must	May	Should not	Must not			
Access-Network-Charging-Identifier-Gx	1022	5.3.22	Grouped	M,V	P			Y	All	CC
Allocation-Retention-Priority	1034	5.3.32	Grouped	M,V	P			Y	All	Both
AN-GW-Address	1050	5.3.49	Address	M, V	P			Y	All	Both
ARP-Value	1046	5.3.45	Unsigned32	M,V	P			Y	All	Both
APN-Aggregate-Max-Bitrate-DL	1040	5.3.39	Unsigned32	M,V	P			Y	3GPP-EPS	PC
APN-Aggregate-Max-Bitrate-UL	1041	5.3.40	Unsigned32	M,V	P			Y	3GPP-EPS	PC
Bearer-Control-Mode	1023	5.3.23	Enumerated	M,V	P			Y	All	PC
Bearer-Identifier	1020	5.3.20	OctetString	M,V	P			Y	3GPP-GPRS	Both
Bearer-Operation	1021	5.3.21	Enumerated	M,V	P			Y	3GPP-GPRS	Both
Bearer-Usage	1000	5.3.1	Enumerated	M,V	P			Y	3GPP-GPRS	Both
Charging-Rule-Install	1001	5.3.2	Grouped	M,V	P			Y	All	Both
Charging-Rule-Remove	1002	5.3.3	Grouped	M,V	P			Y	All	Both
Charging-Rule-Definition	1003	5.3.4	Grouped	M,V	P			Y	All	Both
Charging-Rule-Base-Name	1004	5.3.5	UTF8String	M,V	P			Y	All	Both
Charging-Rule-Name	1005	5.3.6	OctetString	M,V	P			Y	All	Both
Charging-Rule-Report	1018	5.3.18	Grouped	M,V	P			Y	All	Both
CoA-IP-Address	1035	5.3.33	Address	M,V	P			Y	All	Both
CoA-Information	1039	5.3.37	Grouped	M,V	P			Y	All	Both
Event-Report-Indication	1033	5.3.30	Grouped	M,V	P			Y	All	Both
Event-Trigger	1006	5.3.7	Enumerated	M,V	P			Y	All	Both
IP-CAN-Type	1027	5.3.27	Enumerated	M,V	P			Y	All	Both
Guaranteed-Bitrate-DL	1025	5.3.25	Unsigned32	M,V	P			Y	All	PC
Guaranteed-Bitrate-UL	1026	5.3.26	Unsigned32	M,V	P			Y	All	PC
Metering-Method	1007	5.3.8	Enumerated	M,V	P			Y	All	CC
Network-Request-Support	1024	5.3.24	Enumerated	M,V	P			Y	All	PC
Offline	1008	5.3.9	Enumerated	M,V	P			Y	All	CC
Online	1009	5.3.10	Enumerated	M,V	P			Y	All	CC
Precedence	1010	5.3.11	Unsigned32	M,V	P			Y	All	Both
Pre-emption-Capability	1047	5.3.46	Enumerated	M,V	P			Y	3GPP-EPS	Both
Pre-emption-Vulnerability	1048	5.3.47	Enumerated	M,V	P			Y	3GPP-EPS	Both
Reporting-Level	1011	5.3.12	Enumerated	M,V	P			Y	All	CC
PCC-Rule-Status	1019	5.3.19	Enumerated	M,V	P			Y	All	Both
Session-Release-Cause	1045	5.3.44	Enumerated	M,V	P			Y	All	Both
QoS-Class-Identifier	1028	5.3.17	Enumerated	M,V	P			Y	All	Both
QoS-Information	1016	5.3.16	Grouped	M.V	P			Y	All	Both
QoS-Negotiation	1029	5.3.28	Enumerated	M,V	P			Y	3GPP-GPRS 3GPP-EPS	PC
Qos-Upgrade	1030	5.3.29	Enumerated	M.V	P			Y	3GPP-GPRS	PC
Default-EPS-Bearer-QoS	1049	5.3.48	Grouped	M,V	P			Y	NOTE 5	PC
Rule-Failure-Code	1031	5.3.38	Enumerated	M.V	P			Y	All	Both
TFT-Filter	1012	5.3.13	IPFilterRule	M,V	P			Y	3GPP-GPRS	Both
TFT-Packet-Filter-Information	1013	5.3.14	Grouped	M,V	P			Y	3GPP-GPRS	Both
ToS-Traffic-Class	1014	5.3.15	OctetString	M,V	P			Y	3GPP-GPRS	Both
Tunnel-Header-Filter	1036	5.3.34	IPFilterRule	M,V	P			Y	All	Both
Tunnel-Header-Length	1037	5.3.35	Unsigned32	M,V	P			Y	All	Both

Tunnel-Information	1038	5.3.36	Grouped	M,V	P			Y	All	Both
RAT-Type	1032	5.3.31	Enumerated	M,V	P			Y	NOTE 4	Both
Revalidation-Time	1042	5.3.41	Time	M,V	P			Y	All	Both
Rule-Activation-Time	1043	5.3.42	Time	M,V	P			Y	All	Both
Rule-DeActivation-Time	1044	5.3.43	Time	M,V	P			Y	All	Both

NOTE 1: The AVP header bit denoted as 'M', indicates whether support of the AVP is required. The AVP header bit denoted as 'V', indicates whether the optional Vendor-ID field is present in the AVP header. For further details, see RFC 3588 [4].
NOTE 2: The value types are defined in RFC 3588 [4].
NOTE 3: AVPs marked with 'CC' are applicable to charging control, AVPs marked with 'PC' are applicable to policy control and AVPs marked with 'Both' are applicable to both charging control and policy control.
NOTE 4: RAT-Type AVP applies to 3GPP and 3GPP2 access types.
NOTE 5: Default-EPS-Bearer-QoS does not apply for 3GPP-GPRS access type.

5.3.1 Bearer-Usage AVP (3GPP-GPRS access type only)

The Bearer-Usage AVP (AVP code 1000) is of type Enumerated, and it shall indicate how the bearer is being used. If the Bearer-Usage AVP has not been previously provided, its absence shall indicate that no specific information is available. If the Bearer-Usage AVP has been provided, its value shall remain valid until it is provided the next time. The following values are defined:

GENERAL (0)

This value shall indicate no specific bearer usage information is available.

IMS_SIGNALLING (1)

This value shall indicate that the bearer is used for IMS signalling only.

Editor's Note: It is for further study whether this AVP applies to I-WLAN or not.

5.3.2 Charging-Rule-Install AVP (All access types)

The Charging-Rule-Install AVP (AVP code 1001) is of type Grouped, and it is used to activate, install or modify PCC rules as instructed from the PCRF to the PCEF.

For installing a new PCC rule or modifying a PCC rule already installed, Charging-Rule-Definition AVP shall be used.

For activating a specific PCC rule predefined at the PCEF, Charging-Rule-Name AVP shall be used as a reference for that PCC rule. The Charging-Rule-Base-Name AVP is a reference that may be used for activating a group of PCC rules predefined at the PCEF.

For GPRS scenarios where the bearer binding is performed by the PCRF, the Bearer Identifier AVP shall be included as part of Charging-Rule-Install AVP.

If present within Charging-Rule-Install AVP, the Bearer-Identifier AVP indicates that the PCC rules within this Charging-Rule-Install AVP shall be installed or activated within the IP CAN bearer identified by the Bearer-Identifier AVP.

If no Bearer-Identifier AVP is included within the Charging-Rule-Install AVP, the PCEF shall select an IP CAN bearer for each of the PCC rules within this Charging-Rule-Install AVP, were the PCC rule is installed or activated.

If Rule-Activation-Time or Rule-Deactivation-Time is specified then it applies to all the PCC rules within the Charging-Rule-Install

AVP Format:

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

```
                              [ Rule-Activation-Time ]
                              [ Rule-Deactivation-Time ]
                             *[ AVP ]
```

5.3.3 Charging-Rule-Remove AVP (All access types)

The Charging-Rule-Remove AVP (AVP code 1002) is of type Grouped, and it is used to deactivate or remove PCC rules from an IP CAN session.

Charging-Rule-Name AVP is a reference for a specific PCC rule at the PCEF to be removed or for a specific PCC rule predefined at the PCEF to be deactivated. The Charging-Rule-Base-Name AVP is a reference for a group of PCC rules predefined at the PCEF to be deactivated.

AVP Format:

```
Charging-Rule-Remove ::= < AVP Header: 1002 >
                           *[ Charging-Rule-Name ]
                           *[ Charging-Rule-Base-Name ]
                           *[ AVP ]
```

5.3.4 Charging-Rule-Definition AVP (All access types)

The Charging-Rule-Definition AVP (AVP code 1003) is of type Grouped, and it defines the PCC rule for a service flow sent by the PCRF to the PCEF. The Charging-Rule-Name AVP uniquely identifies the PCC rule and it is used to reference to a PCC rule in communication between the PCEF and the PCRF within one IP CAN session. The Flow-Description AVP(s) determines the traffic that belongs to the service flow.

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

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

AVP Format:

```
Charging-Rule-Definition ::= < AVP Header: 1003 >
                              { Charging-Rule-Name }
                              [ Service-Identifier ]
                              [ Rating-Group ]
                             *[ Flow-Description ]
                              [ Flow-Status ]
                              [ QoS-Information ]
                              [ Reporting-Level ]
                              [ Online ]
                              [ Offline ]
                              [ Metering-Method ]
                              [ Precedence ]
                              [ AF-Charging-Identifier ]
                             *[ Flows ]
                             *[ AVP ]
```

5.3.5 Charging-Rule-Base-Name AVP (All access types)

The Charging-Rule-Base-Name AVP (AVP code 1004) is of type UTF8String, and it indicates the name of a pre-defined group of PCC rules residing at the PCEF.

5.3.6 Charging-Rule-Name AVP (All access types)

The Charging-Rule-Name AVP (AVP code 1005) is of type OctetString, and it defines a name for PCC rule. For PCC rules provided by the PCRF it uniquely identifies a PCC rule within one IP CAN session. For PCC rules pre-defined at the PCEF it uniquely identifies a PCC rule within the PCEF.

5.3.7 Event-Trigger AVP (All access types)

The Event-Trigger AVP (AVP code 1006) is of type Enumerated. When sent from the PCRF to the PCEF the Event-Trigger AVP indicates an event that shall cause a re-request of PCC rules. When sent from the PCEF to the PCRF the Event-Trigger AVP indicates that the corresponding event has occurred at the gateway.

NOTE: An exception to the above is the Event Trigger AVP set to NO_EVENT_TRIGGERS, that indicates that PCEF shall not notify PCRF of any event that requires to be provisioned.

NOTE: There are events that do not require to be provisioned by the PCRF, according to the value definition included in this clause. These events will always be reported by the PCEF eventhough the PCRF has not provisioned them in a RAR or CAA command.

Whenever the PCRF subscribes to one or more event triggers by using the RAR command, the PCEF shall send the corresponding currently applicable values (e.g. 3GPP-SGSN-Address AVP or 3GPP-SGSN-IPv6-Address AVP, RAT-Type, 3GPP-User-Location-Info, etc.) to the PCRF in the RAA if available, and in this case, the Event-Trigger AVPs shall not be included.

Whenever one of these events occurs, the PCEF shall send the related AVP that has changed together with the event trigger indication.

Unless stated for a specific value, the Event-Trigger AVP applies to all access types.

The values 8, 9, and 10 are obsolete and shall not be used.

The following values are defined:

SGSN_CHANGE (0)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon the change of the serving SGSN PCC rules shall be requested. When used in a CCR command, this value indicates that the PCEF generated the request because the serving SGSN changed. The new value of the serving SGSN shall be indicated in either 3GPP-SGSN-Address AVP or 3GPP-SGSN-IPv6-Address AVP. Applicable only to 3GPP-GPRS and 3GPP-EPS access types.

QOS_CHANGE (1)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon any QoS change (even within the limits of the current authorization) at bearer or APN level PCC rules shall be requested. When used in a CCR command, this value indicates that the PCEF generated the request because there has been a change in the requested QoS for a specific bearer (e.g. the previously maximum authorized QoS has been exceeded) or APN. The Bearer-Identifier AVP shall be provided to indicate the affected bearer. QoS-Information AVP is required to be provided in the same request with the new value.

NOTE: QoS information at APN level is 3GPP-EPS access specific. See Annex B for further details.

RAT_CHANGE (2)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon a RAT change PCC rules shall be requested. When used in a CCR command, this value indicates that the PCEF generated the request because of a RAT change. The new RAT type shall be provided in the RAT-Type AVP.

TFT_CHANGE (3)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon a TFT change at bearer level PCC rules shall be requested. When used in a CCR command, this value indicates that the PCEF generated the request because of a change in the TFT. The Bearer-Identifier AVP shall be provided to indicate the affected bearer. The new TFT values shall be provided in TFT-Packet-Filter-Information AVP. Applicable only to 3GPP-GPRS.

PLMN_CHANGE (4)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon a PLMN change PCC rules shall be requested. When used in a CCR command, this value indicates that the PCEF generated the request

because there was a change of PLMN. 3GPP-SGSN-MCC-MNC AVP shall be provided in the same request with the new value.

LOSS_OF_BEARER (5)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon loss of bearer, GW should inform PCRF. When used in a CCR command, this value indicates that the PCEF generated the request because the bearer associated with the PCC rules indicated by the corresponding Charging-Rule-Report AVP was lost. The PCC-Rule-Status AVP within the Charging-Rule-Report AVP shall indicate that these PCC rules are temporarily inactive. Applicable to those access-types that handle multiple bearers within one single IP-CAN session (e.g. GPRS).
The mechanism of indicating loss of bearer to the GW is IP-CAN access type specific. For GPRS, this is indicated by a PDP context modification request with Maximum Bit Rate (MBR) in QoS profile changed to 0 kbps.
When the PCRF performs the bearer binding, the PCEF shall provide the Bearer-Identifier AVP to indicate the bearer that has been lost.

RECOVERY_OF_BEARER (6)

This value shall be in CCA and RAR commands by the PCRF used to indicate that upon recovery of bearer, GW should inform PCRF. When used in a CCR command, this value indicates that the PCEF generated the request because the bearer associated with the PCC rules indicated by the corresponding Charging-Rule-Report AVP was recovered. The PCC-Rule-Status AVP within the Charging-Rule-Report AVP shall indicate that these rules are active again. Applicable to those access-types that handle multiple bearers within one single IP-CAN session (e.g. GPRS).
The mechanism for indicating recovery of bearer to the GW is IP-CAN access type specific. For GPRS, this is indicated by a PDP context modification request with Maximum Bit Rate (MBR) in QoS profile changed from 0 kbps to a valid value.
When the PCRF performs the bearer binding, the PCEF shall provide the Bearer-Identifier AVP to indicate the bearer that has been recovered.

IP-CAN_CHANGE (7)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon a change in the IP-CAN type PCC rules shall be requested. When used in a CCR command, this value indicates that the PCEF generated the request because there was a change of IP-CAN type. IP-CAN-Type AVP shall be provided in the same request with the new value., The RAT-Type AVP shall also be provided when applicable to the specific IP-CAN Type (e.g. 3GPP IP-CAN Type)

QOS_CHANGE_EXCEEDING_AUTHORIZATION (11)

This value shall be used in CCA and RAR commands by the PCRF to indicate that only upon a requested QoS change beyond the current authorized value(s) at bearer level PCC rules shall be requested. When used in a CCR command, this value indicates that the PCEF generated the request because there has been a change in the requested QoS beyond the authorized value(s) for a specific bearer. The Bearer-Identifier AVP shall be provided to indicate the affected bearer. QoS-Information AVP is required to be provided in the same request with the new value.

RAI_CHANGE (12)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon a change in the RAI, PCEF shall inform the PCRF. When used in a CCR command, this value indicates that the PCEF generated the request because there has been a change in the RAI. The new RAI value shall be provided in the RAI AVP. If the user location has been changed but the PCEF can not get the detail location information for some reasons (eg. handover from 3G to 2G network), the PCEF shall send the RAI AVP to the PCRF by setting the LAC of the RAI to value 0x0000. Applicable only to 3GPP-GPRS and 3GPP-EPS access types.

USER_LOCATION_CHANGE (13)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon a change in the user location, PCEF shall inform the PCRF. When used in a CCR command, this value indicates that the PCEF generated the request because there has been a change in the user location. The new location value shall be provided in the 3GPP-User-Location-Info AVP. If the user location has been changed but the PCEF can not get the detail location information for some reasons (eg. handover from 3G to 2G network), the PCEF shall send the

3GPP-User-Location-Info AVP to the PCRF by setting the LAC of the CGI/SAI to value 0x0000. Applicable only to 3GPP-GPRS and 3GPP-EPS access types..

NO_EVENT_TRIGGERS (14)

This value shall be used in CCA and RAR commands by the PCRF to indicate that PCRF does not require any Event Trigger notification.

OUT_OF_CREDIT (15)

This value shall be used in CCA and RAR commands by the PCRF to indicate that the PCEF shall inform the PCRF about the PCC rules for which credit is no longer available, together with the applied termination action. When used in a CCR command, this value indicates that the PCEF generated the request because the PCC rules indicated by the corresponding Charging-Rule-Report AVP have run out of credit, and that the termination action indicated by the corresponding Final-Unit-Indication AVP applies applies (3GPP TS 32.240 [21] and 3GPP TS 32.299 [19]).

REALLOCATION_OF_CREDIT (16)

This value shall be used in CCA and RAR commands by the PCRF to indicate that the PCEF shall inform the PCRF about the PCC rules for which credit has been reallocated after the former out of credit indication. When used in a CCR command, this value indicates that the PCEF generated the request because the PCC rules indicated by the corresponding Charging-Rule-Report AVP have been reallocated credit after the former out of credit indication (3GPP TS 32.240 [21] and 3GPP TS 32.299 [19]).
REVALIDATION_TIMEOUT(17)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon revalidation timeout, PCEF shall inform the PCRF. When used in a CCR command, this value indicates that the PCEF generated the request because there has been a PCC revalidation timeout.

UE_IP_ADDRESS_ALLOCATE (18)

This value may be used in CCA and RAR commands by the PCRF to indicate that the PCEF shall inform the PCRF upon an IPv4 address allocation, When used in a CCR command, this value indicates that the PCEF generated the request because a UE IPv4 address is allocated. The Framed-IP-Address AVP shall be provided in the same request. This event trigger does not require to be provisioned by the PCRF.

UE_IP_ADDRESS_RELEASE (19)

This value may be used in CCA and RAR commands by the PCRF to indicate that the PCEF shall inform the PCRF upon an IPv4 address release, When used in a CCR command, this value shall be used in a CCR command to indicate that the PCEF generated the request because a UE IPv4 address is released. The Framed-IP-Address AVP shall be provided in the same request. This event trigger does not require to be provisioned by the PCRF.

DEFAULT_EPS_BEARER_QOS_CHANGE (20)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon a change in the default EPS Bearer QoS, PCEF shall inform the PCRF. When used in a CCR command, this value indicates that the PCEF generated the request because there has been a change in the default EPS Bearer QoS. The new value shall be provided in the Default-EPS-Bearer-QoS AVP. Not applicable in 3GPP-GPRS access type.

AN_GW_CHANGE (21)

This value shall be used in CCA and RAR commands by the PCRF to indicate that upon the change of the serving Access Node Gateway, PCC rules shall be requested. When used in a CCR command, this value indicates that the PCEF generated the request because the serving Access Node gateway changed. The new value of the serving Access Node gateway shall be indicated in the AN-GW-Address AVP.

5.3.8 Metering-Method AVP (All access types)

The Metering-Method AVP (AVP code 1007) is of type Enumerated, and it defines what parameters shall be metered for offline charging. The PCEF may use the AVP for online charging in case of decentralized unit determination, refer to 3GPP TS 32.299 [19].

The following values are defined:

DURATION (0)

This value shall be used to indicate that the duration of the service flow shall be metered.

VOLUME (1)

This value shall be used to indicate that volume of the service flow traffic shall be metered.

DURATION_VOLUME (2)

This value shall be used to indicate that the duration and the volume of the service flow traffic shall be metered.

If the Metering-Method AVP is omitted but has been supplied previously, the previous information remains valid. If the Metering-Method AVP is omitted and has not been supplied previously, the metering method pre-configured at the PCEF is applicable as default metering method.

5.3.9 Offline AVP (All access types)

The Offline AVP (AVP code 1008) is of type Enumerated.

If the Offline AVP is embedded within a Charging_Rule-Definition AVP it defines whether the offline charging interface from the PCEF for the associated PCC rule shall be enabled. The absence of this AVP within the first provisioning of the Charging-Rule-definition AVP of a new PCC rule indicates that the default charging method for offline shall be used.

If the Offline AVP is embedded within the initial CCR on command level, it indicates the default charging method for offline pre-configured at the PCEF is applicable as default charging method for offline. The absence of this AVP within the initial CCR indicates that the charging method for offline pre-configured at the PCEF is not available.

If the Offline AVP is embedded within the initial CCA on command level, it indicates the default charging method for offline. The absence of this AVP within the initial CCA indicates that the charging method for offline pre-configured at the PCEF is applicable as default charging method for offline.

The default charging method provided by the PCRF shall take precedence over any pre-configured default charging method at the PCEF.

The following values are defined:

DISABLE_OFFLINE (0)

This value shall be used to indicate that the offline charging interface for the associated PCC rule shall be disabled.

ENABLE_OFFLINE (1)

This value shall be used to indicate that the offline charging interface for the associated PCC rule shall be enabled.

5.3.10 Online AVP (All access types)

The Online AVP (AVP code 1009) is of type Enumerated.

If the Online AVP is embedded within a Charging_Rule-Definition AVP, it defines whether the online charging interface from the PCEF for the associated PCC rule shall be enabled. The absence of this AVP within the first provisioning of the Charging-Rule-Definition AVP of a new PCC rule indicates that the default charging method for online shall be used.

If the Online AVP is embedded within the initial CCR on command level, it indicates the default charging method for online pre-configured at the PCEF is applicable as default charging method for online. The absence of this AVP within the initial CCR indicates that the charging method for online pre-configured at the PCEF is not available.

If the Online AVP is embedded within the initial CCA on command level, it indicates the default charging method for online. The absence of this AVP within the initial CCA indicates that the charging method for online pre-configured at the PCEF is applicable as default charging method for online.

The default charging method provided by the PCRF shall take precedence over any pre-configured default charging method at the PCEF.

The following values are defined:

DISABLE_ONLINE (0)

This value shall be used to indicate that the online charging interface for the associated PCC rule shall be disabled.

ENABLE_ONLINE (1)

This value shall be used to indicate that the online charging interface for the associated PCC rule shall be enabled.

5.3.11 Precedence AVP (All access types)

The Precedence AVP (AVP code 1010) is of type Unsigned32.

Within the Charging Rule Definition AVP, the Precedence AVP determines the order, in which the service data flow templates are applied at service data flow detection at the PCEF. A PCC rule with the Precedence AVP with lower value shall be applied before a PCC rule with the Precedence AVP with higher value.

NOTE: For PCRF-initiated IP-CAN session modification cases where the PCEF creates new service data flow filters (eg. new TFT-UL filters), the PCEF need to make an appropriate mapping between the value of the Precedence AVP from the PCC rule and the precedence information of the service data flow filter. The PCEF have to maintain the order of the precedence information provided by the PCRF with the precedence information of the new service data flow filters.

The Precedence AVP is also used within the TFT-Packet-Filter-Information AVP to indicate the evaluation precedence of the Traffic Mapping Information filters (for GPRS the TFT packet filters) as received from the UE. The PCEF shall assign a lower value in the corresponding Precedence AVP to a Traffic Mapping Information filter with a higher evaluation precedence than to a Traffic Mapping Information filter with a lower evaluation precedence.

5.3.12 Reporting-Level AVP (All access types)

The Reporting-Level AVP (AVP code 1011) is of type Enumerated, and it defines on what level the PCEF reports the usage for the related PCC rule. The following values are defined:

SERVICE_IDENTIFIER_LEVEL (0)

This value shall be used to indicate that the usage shall be reported on service id and rating group combination level.

RATING_GROUP_LEVEL (1)

This value shall be used to indicate that the usage shall be reported on rating group level.

If the Reporting-Level AVP is omitted but has been supplied previously, the previous information remains valid. If the Reporting-Level AVP is omitted and has not been supplied previously, the reporting level pre-configured at the PCEF is applicable as default reporting level.

5.3.13 TFT-Filter AVP (3GPP-GPRS access type only)

The TFT-Filter AVP (AVP code 1012) is of type IPFilterRule, and it contains the flow filter for one TFT packet filter. The TFT-Filter AVP is derived from the Traffic Flow Template (TFT) defined in 3GPP TS 24.008 [13]. The following information shall be sent:

- Action shall be set to "permit".
- Direction shall be set to "out".
- Protocol shall be set to the value provided within the TFT packet filter parameter "Protocol Identifier/Next Header Type". If the TFT packet filter parameter "Protocol Identifier/Next Header Type" is not provided within the TFT packet filter, Protocol shall be set to "ip".
- Source IP address (possibly masked). The source IP address shall be derived from TFT packet filter parameters "Source address" and "Subnet Mask". The source IP address shall be set to "any", if no such information is provided in the TFT packet filter.
- Source and destination port (single value, list or ranges). The information shall be derived from the corresponding TFT packet filter parameters. Source and/or destination port(s) shall be omitted if such information is not provided in the TFT packet filter.
- The Destination IP address shall be set to "assigned".

The IPFilterRule type shall be used with the following restrictions:

- No options shall be used.
- The invert modifier "!" for addresses shall not be used.

The direction "out" refers to downlink direction.

5.3.14 TFT-Packet-Filter-Information AVP (3GPP-GPRS access type only)

The TFT-Packet-Filter-Information AVP (AVP code 1013) is of type Grouped, and it contains the information from a single TFT packet filter including the evaluation precedence, the filter and the Type-of-Service/Traffic Class sent from the PCEF to the PCRF. The PCEF shall include one TFT-Packet-Filter-Information AVP for each TFT packet filters applicable at a PDP context in separate TFT-Packet-Filter-Information AVPs within each PCC rule request. corresponding to that PDP context. TFT-Packet-Filter-Information AVPs are derived from the Traffic Flow Template (TFT) defined in 3GPP TS 24.008 [13].

AVP Format:

```
TFT-Packet-Filter-Information ::= < AVP Header: 1013 >
                              [ Precedence ]
                              [ TFT-Filter ]
                              [ ToS-Traffic-Class ]
```

5.3.15 ToS-Traffic-Class AVP (3GPP-GPRS access type only)

The ToS-Traffic-Class AVP (AVP code 1014) is of type OctetString, and it contains the Type-of-Service/Traffic-Class of a TFT packet filter as defined in 3GPP TS 24.008 [13].

5.3.16 QoS-Information AVP (All access types)

The QoS-Information AVP (AVP code 1016) is of type Grouped, and it defines the QoS information for an IP-CAN bearer, PCC rule, QCI or APN. When this AVP is sent from the PCEF to the PCRF, it indicates the requested QoS information for an IP CAN bearer or the subscribed QoS information at APN level. When this AVP is sent from the PCRF to the PCEF, it indicates the authorized QoS for:

- an IP CAN bearer (when appearing at CCA or RAR command level or
- a service flow (when included within the PCC rule) or

- a QCI (when appearing at CCA or RAR command level with the QoS-Class-Identifier AVP and the Maximum-Requested-Bandwidth-UL AVP and/or the Maximum-Requested-Bandwidth-DL AVP) or

- an APN (when appearing at CCA or RAR command level with APN-Aggregate-Max-Bitrate-DL and APN-Aggregate-Max-Bitrate-DL).

The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS, excluding the applicable bitrates and ARP. It is applicable both for uplink and downlink direction.

The Max-Requested-Bandwidth-UL defines the maximum bit rate allowed for the uplink direction.

The Max-Requested-Bandwidth-DL defines the maximum bit rate allowed for the downlink direction.

The Guaranteed-Bitrate-UL defines the guaranteed bit rate allowed for the uplink direction.

The Guaranteed-Bitrate-DL defines the guaranteed bit rate allowed for the downlink direction.

The APN-Aggregate-Max-Bitrate-UL defines the total bandwidth usage for the uplink direction of non-GBR QCIs at the APN. This AVP only applies to 3GPP-EPS access.

The APN-Aggregate-Max-Bitrate-DL defines the total bandwidth usage for the downlink direction of non-GBR QCIs at the APN. This AVP only applies to 3GPP-EPS access.

The Bearer Identifier AVP shall be included as part of the QoS-Information AVP if the QoS information refers to an IP CAN bearer initiated by the UE and the PCRF performs the bearer binding. The Bearer Identifier AVP identifies this bearer. Several QoS-Information AVPs for different Bearer Identifiers may be provided per command.

The Allocation-Retention-Priority AVP is an indicator of the priority of allocation and retention for the Service Data Flow.

If the QoS-Information AVP has been supplied previously but is omitted in a Diameter message or AVP, the previous information remains valid. If the QoS-Information AVP has not been supplied from the PCRF to the PCEF previously and is omitted in a Diameter message or AVP, no enforcement of the authorized QoS shall be performed.

AVP Format:

```
QoS-Information ::=     < AVP Header: 1016 >
                      [ QoS-Class-Identifier ]
                      [ Max-Requested-Bandwidth-UL ]
                      [ Max-Requested-Bandwidth-DL ]
                      [ Guaranteed-Bitrate-UL ]
                      [ Guaranteed-Bitrate-DL ]
                      [ Bearer-Identifier ]
                      [ Allocation-Retention-Priority]
                      [ APN-Aggregate-Max-Bitrate-UL]
                      [ APN-Aggregate-Max-Bitrate-DL]
                    * [AVP]
```

5.3.17 QoS-Class-Identifier AVP (All access types)

QoS-Class-Identifier AVP (AVP code 1028) is of type Enumerated, and it identifies a set of IP-CAN specific QoS parameters that define the authorized QoS, excluding the applicable bitrates and ARP for the IP-CAN bearer or service flow. The following values are defined:

Table 5.3.17.1: Void

5.3.18 Charging-Rule-Report AVP (All access types)

The Charging-Rule-Report AVP (AVP code 1018) is of type Grouped, and it is used to report the status of PCC rules.

Charging-Rule-Name AVP is a reference for a specific PCC rule at the PCEF that has been successfully installed, modified or removed (for dynamic PCC rules), or activated or deactivated (for predefined PCC rules) because of trigger from the MS. Charging-Rule-Base-Name AVP is a reference for a group of PCC rules predefined at the PCEF that has been successfully activated or deactivated because of trigger from the MS.

The Charging-Rule-Report AVP can also be used to report the status of the PCC rules which cannot be installed/activated or enforced at the PCEF. In this condition, the Charging-Rule-Name AVP is used to indicate a

specific PCC rule which cannot be installed/activated or enforced, and the Charging-Rule-Base-Name AVP is used to indicate a group of PCC rules which cannot be activated. The Rule-Failure-Code indicates the reason that the PCC rules cannot be successfully installed/activated or enforced.

The Charging-Rule-Report AVP can also be used to report the status of the PCC rules for which credit is no longer available or credit has been reallocated after the former out of credit indication. When reporting an out of credit condition, the Final-Unit-Indication AVP indicates the termination action the PCEF applies to the PCC rules as instructed by the OCS.

AVP Format:

```
Charging-Rule-Report ::= < AVP Header: 1018 >
                         *[Charging-Rule-Name]
                         *[Charging-Rule-Base-Name]
                          [PCC-Rule-Status]
                          [Rule-Failure-Code]
                          [Final-Unit-Indication]
                         *[AVP]
```

Multiple instances of Charging-Rule-Report AVPs shall be used in the case it is required to report different PCC-Rule-Status or Rule-Failure-Code values for different groups of rules within the same Diameter command.

5.3.19 PCC-Rule-Status AVP (All access types)

The PCC-Rule-Status AVP (AVP code 1019) is of type Enumerated, and describes the status of one or a group of PCC Rules.

The following values are defined:

ACTIVE (0)

This value is used to indicate that the PCC rule(s) are successfuly installed (for those provisioned from PCRF) or activated (for those pre-provisioned in PCEF)

INACTIVE (1)

This value is used to indicate that the PCC rule(s) are removed (for those provisioned from PCRF) or inactive (for those pre-provisioned in PCEF)

TEMPORARILY INACTIVE (2)

This value is used to indicate that, for some reason (e.g. loss of bearer), already installed or activated PCC rules are temporarily disabled.

5.3.20 Bearer-Identifier AVP (Applicable access type 3GPP-GPRS)

The Bearer-Identifier AVP (AVP code 1020) is of type OctetString, and it indicates the bearer to which specific information refers.

When present within a CC-Request Diameter command, subsequent AVPs within the CC-Request refer to the specific bearer identified by this AVP.

The bearer identifier of an IP CAN bearer shall be unique within the corresponding IP CAN session. The bearer identifier shall be selected by the PCEF.

5.3.21 Bearer-Operation AVP (Applicable access type 3GPP-GPRS)

The Bearer-Operation AVP (AVP code 1021) is of type of Enumerated, and it indicates the bearer event that causes a request for PCC rules. This AVP shall be supplied if the bearer event relates to an IP CAN bearer initiated by the UE.

The following values are defined:

TERMINATION (0)

This value is used to indicate that a bearer is being terminated.

ESTABLISHMENT (1)

This value is used to indicate that a new bearer is being established.

MODIFICATION (2)

This value is used to indicate that an existing bearer is being modified.

5.3.22 Access-Network-Charging-Identifier-Gx AVP (All access types)

The Access-Network-Charging-Identifier-Gx AVP (AVP code 1022) is of type Grouped. It contains a charging identifier (e.g. GCID) within the Access-Network-Charging-Identifier-Value AVP and the related PCC rule name(s) within the Charging-Rule-Name AVP(s). If the IP CAN session contains only a single IP CAN bearer, no Charging-Rule-Name AVPs or Charging-Rule-Base-Name AVPs need to be provided. Otherwise, all the Charging-Rule-Name AVPs or Charging-Rule-Base-Name AVPs corresponding to PCC rules activated or installed within the IP CAN bearer corresponding to the provided Access-Network-Charging-Identifier-Value shall be included.

The Access-Network-Charging-Identifier-Gx AVP can be sent from the PCEF to the PCRF. The PCRF may use this information for charging correlation towards the AF.

AVP Format:

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

5.3.23 Bearer-Control-Mode AVP

The Bearer-Control-Mode AVP (AVP code 1023) is of type of Enumerated. It is sent from PCRF to PCEF and indicates the PCRF selected bearer control mode.

The following values are defined:

UE_ONLY (0)

This value is used to indicate that the UE shall request any resource establishment, modification or termination.

RESERVED (1)

This value is not used in this Release.

UE_NW (2)

This value is used to indicate that both the UE and PCEF may request any resource establishment, modification or termination by adding, modifying or removing traffic flow information.

See Annex A.3.8 for particularities in 3GPP-GPRS access.

5.3.24 Network-Request-Support AVP

The Network-Request-Support AVP (AVP code 1024) is of type of Enumerated and indicates the UE and network support of the network initiated procedures.

If the Network Request Support AVP has not been previously provided, its absence shall indicate the value NETWORK_REQUEST NOT SUPPORTED. If the Network Request Support AVP has been provided, its value shall remain valid until it is provided the next time.

The following values are defined:

NETWORK_REQUEST NOT SUPPORTED (0)

This value is used to indicate that the UE and the access network do not support the network initiated bearer establishment request procedure.

NETWORK_REQUEST SUPPORTED (1)

This value is used to indicate that the UE and the access network support the network initiated bearer establishment request procedure.

5.3.25 Guaranteed-Bitrate-DL AVP

The Guaranteed-Bitrate-DL AVP (AVP code 1025) is of type Unsigned32, and it indicates the guaranteed bitrate in bits per second for a downlink service data flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

5.3.26 Guaranteed-Bitrate-UL AVP

The Guaranteed –Bitrate-UL AVP (AVP code 1026) is of type Unsigned32, and it indicates the guaranteed bitrate in bits per second for an uplink service data flow. The bandwidth contains all the overhead coming from the IP-layer and the layers above, e.g. IP, UDP, RTP and RTP payload.

5.3.27 IP-CAN-Type AVP (All access types)

The IP-CAN-Type AVP (AVP code 1027) is of type Enumerated, and it shall indicate the type of Connectivity Access Network in which the user is connected.

The IP-CAN-Type AVP shall always be present during the IP-CAN session establishment. During an IP-CAN session modification, this AVP shall be present when there has been a change in the IP-CAN type and the PCRF requested to be informed of this event. The Event-Trigger AVP with value IP-CAN CHANGE shall be provided together with the IP-CAN-Type AVP.

The following values are defined:

3GPP-GPRS (0)

This value shall be used to indicate that the IP-CAN is associated with a 3GPP GPRS access and is further detailed by the RAT-Type AVP. RAT-Type AVP will include applicable 3GPP values, except EUTRAN.

DOCSIS (1)

This value shall be used to indicate that the IP-CAN is associated with a DOCSIS access.

xDSL (2)

This value shall be used to indicate that the IP-CAN is associated with an xDSL access.

WiMAX (3)

This value shall be used to indicate that the IP-CAN is associated with a WiMAX access (IEEE 802.16).

3GPP2 (4)

This value shall be used to indicate that the IP-CAN is associated with a 3GPP2 access and is further detailed by the RAT-Type AVP.

3GPP-EPS (5)

This value shall be used to indicate that the IP-CAN associated with a 3GPP EPS access and is further detailed by the RAT-Type AVP.

5.3.28 QoS-Negotiation AVP (3GPP-GPRS and 3GPP-EPS Access Types only)

The QoS-Negotiation AVP (AVP code 1029) is of type Enumerated. The value of the AVP indicates for a single PCC rule request if the PCRF is allowed to negotiate the QoS by supplying in the answer to this request an authorized QoS different from the requested QoS.

The following values are defined:

NO_QoS_NEGOTIATION (0)

This value indicates that a QoS negotiation is not allowed for the corresponding PCC rule request.

QoS_NEGOTIATION_SUPPORTED (1)

This value indicates that a QoS negotiation is allowed for the corresponding PCC rule request. This is the default value applicable if this AVP is not supplied

5.3.29 QoS-Upgrade AVP (3GPP-GPRS Access Type only)

The QoS-Upgrade AVP (AVP code 1030) is of type Enumerated. The value of the AVP indicates whether the SGSN supports that the GGSN upgrades the QoS in a Create PDP context response or Update PDP context response. If the SGSN does not support a QoS upgrade, the PCRF shall not provision an authorized QoS which is higher than the requested QoS for this IP CAN bearer. The setting is applicable to the bearer indicated in the request within the Bearer-Identifier AVP.

If no QoS-Upgrade AVP has been supplied for an IP CAN bearer, the default value QoS_UPGRADE_NOT_SUPPORTED is applicable. If the QoS-Upgrade AVP has previously been supplied for an IP CAN bearer but is not supplied in a new PCC rule request, the previously supplied value remains applicable.

The following values are defined:

QoS_UPGRADE_NOT_SUPPORTED (0)

This value indicates that the IP-CAN bearer does not support the upgrading of the requested QoS. This is the default value applicable if no QoS-Upgrade AVP has been supplied for an IP CAN bearer.

QoS_UPGRADE_SUPPORTED (1)

This value indicates that the IP-CAN bearer supports the upgrading of the requested QoS.

5.3.30 Event-Report-Indication AVP (All access types)

The Event-Report-Indication AVP (AVP code 1033) is of type Grouped. When sent from the PCRF to the PCEF, it is used to report an event coming from the Access NetworkGW(BBERF) and relevant info to the PCEF. When sent from the PCEF to the PCRF, it is used to provide the information about the required event triggers to the PCRF. Only Event-Trigger AVP will be supplied in this case.

The PCEF may require the subscription to new event triggers or the removal of the already subscribed ones. In order to do so, the PCEF shall provide the new complete list of applicable event triggers in the corresponding CCR command.

AVP Format:

```
Event-Report-Indication ::= < AVP Header: 1033 >
                          *[Event-Trigger]
                           [RAT-Type]
                          *[AVP]
```

Editor"s Note: Other relevant information to be added as part of the Event-Report-Indication AVP is FFS.

Editor"s Note: It is FFS if Event-Report-Information AVP can also be used to report an event coming from the PCEF and relevant info to the BBERF.

5.3.31 RAT-Type AVP

The RAT-Type AVP (AVP code 1032) is of type Enumerated and is used to identify the radio access technology that is serving the UE.

NOTE1: Values 0-999 are used for generic radio access technologies that can apply to different IP-CAN types and are not IP-CAN specific.

NOTE2: Values 1000-1999 are used for 3GPP specific radio access technology types.

NOTE3: Values 2000-2999 are used for 3GPP2 specific radio access technology types.

The following values are defined:

WLAN (0)

This value shall be used to indicate that the RAT is WLAN.

UTRAN (1000)

This value shall be used to indicate that the RAT is UTRAN. For further details refer to 3GPP TS 29.060 [18].

GERAN (1001)

This value shall be used to indicate that the RAT is GERAN. For further details refer to 3GPP TS 29.060 [18].

GAN (1002)

This value shall be used to indicate that the RAT is GAN. For further details refer to 3GPP TS 29.060 [18].

HSPA_EVOLUTION (1003)

This value shall be used to indicate that the RAT is HSPA Evolution. For further details refer to 3GPP TS 29.060 [18].

EUTRAN (1004)

This value shall be used to indicate that the RAT is EUTRAN. For further details refer to 3GPP TS 29.274 [22]

CDMA2000_1X (2000)

This value shall be used to indicate that the RAT is CDMA2000 1X. For further details refer to 3GPP2 X.S0011-D [20].

HRPD (2001)

This value shall be used to indicate that the RAT is HRPD. For further details refer to 3GPP2 X.S0011-D [20].

UMB (2002)

This value shall be used to indicate that the RAT is UMB. For further details refer to 3GPP2 X.S0011-D [20].

5.3.32 Allocation-Retention-Priority AVP (All access types)

The Allocation-Retention-Priority AVP (AVP code 1034) is of type Grouped, and it is used to indicate the priority of allocation and retention, the pre-emption capability and pre-emption vulnerability for the SDF if provided within the QoS-Information-AVP or for the EPS default bearer if provided within the Default-EPS-Bearer-QoS AVP.

To prevent unexpected PDN disconnection or UE detach from the network, the PCRF shall set the ARP of the default bearer. The PCRF:

- should set the ARP-value AVP of the default bearer to the highest level of priority;
- shall set the pre-emption-capability AVP of the default bearer to PRE-EMPTION_CAPABILITY_ENABLED per subclause 5.3.46; and
- shall set the pre-emption-vulnerability AVP of the default bearer to PRE-EMPTION_VULNERABILITY_DISABLED per subclause 5.3.47.

NOTE: For the default bearer the ARP-value AVP can be set to 1 per subclause 5.3.45.

AVP Format:

```
Allocation-Retention-Priority ::= < AVP Header: 1034 >
                                  {ARP-Value}
                                  [Pre-emption-Capability]
                                  [Pre-emption-Vulnerability]
```

Editor"s note: Actual values are pending to be defined

5.3.33 CoA-IP-Address AVP (All access types)

The CoA-IP-Address AVP (AVP Code 1035) is of type Address and contains the mobile node"s care-of-address. The care-of-address type may be IPv4 or IPv6.

5.3.34 Tunnel-Header-Filter AVP (All access types)

The Tunnel-Header-Filter AVP (AVP code 1036) is of type IPFilterRule, and it defines the tunnel (outer) header filter information of a MIP tunnel where the associoated QoS rules apply for the tunnel payload.

The Tunnel-Header-Filter AVP shall include the following information:

- Action shall be set to "permit";
- Direction (in or out);
- Protocol
- Source IP address;.
- Source port (single value) for UDP tunneling;
- Destination IP address;
- Destination port (single value) for UDP tunneling.

The IPFilterRule type shall be used with the following restrictions:

- Options shall not be used.
- The invert modifier "!" for addresses shall not be used.

The direction "out" refers to downlink direction.

The direction "in" refers to uplink direction.

5.3.35 Tunnel-Header-Length AVP (All access types)

The Tunnel-Header-Length AVP (AVP code 1037) is of type Unsigned32. This AVP indicates the length of the tunnel header in octets.

5.3.36 Tunnel-Information AVP (All access types)

The Tunnel-Information AVP (AVP code 1038) is of type Grouped, and it contains the tunnel (outer) header information from a single IP flow. The Tunnel-Information AVP is sent from the PCEF to the PCRF and from the PCRF to the BBERF.

The Tunnel-Information AVP may include only the Tunnel-Header-Length AVP, only the Tunnel-Header-Filter AVP, or both.

The Tunnel-Header-Length AVP provides the length of the tunnel header and identifies the offset where the tunneled payload starts. The BBERF uses the length value provided in Tunnel-Header-Length AVP to locate the inner IP header and perform service data flow detection and related QoS control.

The Tunnel-Header-Filter AVP identifies the tunnel (outer) header information in the downlink and uplink directions.

AVP Format:

```
Tunnel-Information ::= < AVP Header: 1038 >
                            [ Tunnel-Header-Length ]
                           2[ Tunnel-Header-Filter ]
                            *[ AVP ]
```

5.3.37 CoA-Information AVP (All access types)

The CoA-Information AVP (AVP code 1039) is of type Grouped, and it contains care-of-address and the tunnel information related to the care of address. The CoA-Information AVP is sent from the PCEF to the PCRF.

When used, the CoA-Information AVP shall include a CoA-IP-Address AVP. The CoA-Information AVP shall also include a Tunnel-Information AVP, which provides the tunnel header length and tunnel header filter information related to the specific care-of-address.

AVP Format:

```
CoA-Information ::= < AVP Header: 1033 >
                            { Tunnel-Information }
                            { CoA-IP-Address }
                           *[AVP]
```

5.3.38 Rule-Failure-Code AVP (All access types)

The Rule-Failure-Code AVP (AVP code 1031) is of type Enumerated. It is sent by the PCEF to the PCRF within a Charging-Rule-Report AVP to identify the reason a PCC Rule is being reported.

The following values are defined:

UNKNOWN_RULE_NAME (1)

This value is used to indicate that the pre-provisioned PCC rule could not be successfully activated because the Charging-Rule-Name or Charging-Rule-Base-Name is unknown to the PCEF.

RATING_GROUP_ERROR (2)

This value is used to indicate that the PCC rule could not be successfully installed or enforced because the Rating-Group specified within the Charging-Rule-Definition AVP by the PCRF is unknown or, invalid.

SERVICE_IDENTIFIER_ERROR (3)

This value is used to indicate that the PCC rule could not be successfully installed or enforced because the Service-Identifier specified within the Charging-Rule-Definition AVP by the PCRF is invalid, unknown, or not applicable to the service being charged.

GW/PCEF_MALFUNCTION (4)

This value is used to indicate that the PCC rule could not be successfully installed (for those provisioned from the PCRF) or activated (for those pre-provisioned in PCEF) or enforced (for those already successfully installed) due to GW/PCEF malfunction.

RESOURCES_LIMITATION (5)

This value is used to indicate that the PCC rule could not be successfully installed (for those provisioned from PCRF) or activated (for those pre-provisioned in PCEF) or enforced (for those already successfully installed) due to a limitation of resources at the PCEF.

MAX_NR_BEARERS_REACHED (6)

This value is used to indicate that the PCC rule could not be successfully installed (for those provisioned from PCRF) or activated (for those pre-provisioned in PCEF) or enforced (for those already successfully installed) due to the fact that the maximum number of bearers has been reached for the IP-CAN session.

UNKNOWN_BEARER_ID (7)

This value is used to indicate that the PCC rule could not be successfully installed or enforced at the PCEF because the Bearer-Id specified within the Charging-Rule-Install AVP by the PCRF is unknown or invalid. Applicable only for GPRS in the case the PCRF performs the bearer binding.

MISSING_BEARER_ID (8)

This value is used to indicate that the PCC rule could not be successfully installed or enforced at the PCEF because the Bearer-Id is not specified within the Charging-Rule-Install AVP by the PCRF. Applicable only for GPRS in the case the PCRF performs the bearer binding.

MISSING_FLOW_DESCRIPTION (9)

This value is used to indicate that the PCC rule could not be successfully installed or enforced because the Flow-Description AVP is not specified within the Charging-Rule-Definition AVP by the PCRF during the first install request of the PCC rule.

5.3.39 APN-Agreggate-Max-Bitrate-DL AVP (Applicable access type 3GPP-EPS)

The APN-Aggregated-Max-Bitrate-DL AVP (AVP code 1040) is of type Unsigned32, and it indicates the maximum aggregate bit rate in bits per seconds for the downlink direction across all non-GBR bearers related with the same APN.

When provided in a CC-Request, it indicates the subscribed maximum bitrate. When provided in a CC-Answer, it indicates the maximum bandwidth authorized by PCRF.

5.3.40 APN-Agreggate-Max-Bitrate-UL AVP (Applicable access type 3GPP-EPS)

The APN-Aggregated-Max-Bitrate-UL AVP (AVP code 1041) is of type Unsigned32, and it indicates the maximum aggregate bit rate in bits per seconds for the uplink direction across all non-GBR bearers related with the same APN.

When provided in a CC-Request, it indicates the subscribed maximum bandwidth. When provided in a CC-Answer, it indicates the maximum bandwidth authorized by PCRF.

5.3.41 Revalidation-Time (ALL Access Types)

The Revalidation-Time AVP (AVP code 1042) is of type Time. This value indicates the NTP time before which the PCEF will have to re-request PCC rules. This value shall be provided with the event trigger when REVALIDATION_TIMEOUT is provisioned via CCA or RAR.

5.3.42 Rule-Activation-Time (ALL Access Types)

The Rule-Activation-Time AVP (AVP code 1043) is of type Time. This value indicates the NTP time at which the PCC rule has to be enforced. The AVP is included in Charging-Rule-Install AVP and is applicable for all the PCC rules included within the Charging-Rule-Install AVP

5.3.43 Rule-Deactivation-Time (ALL Access Types)

The Rule-Deactivation-Time AVP (AVP code 1044) is of type Time. This value indicates the NTP time at which the PCEF has to stop enforcing the PCC rule . The AVP is included in Charging-Rule-Install AVP and is applicable for all the PCC rules included within the Charging-Rule-Install AVP

5.3.44 Session-Release-Cause (All access types)

Session-Release-Cause AVP (AVP code 1045) is of type Enumerated, and determines the cause of release the IP-CAN session by the PCRF. The following values are defined:

UNSPECIFIED_REASON (0)

This value is used for unspecified reasons.

UE_SUBSCRIPTION_REASON (1)

This value is used to indicate that the subscription of UE has changed (e.g. removed) and the session needs to be terminated.

INSUFFICIENT_SERVER_RESOURCES (2)

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

5.3.45 ARP-Value AVP (All access types)

The ARP-Value AVP (AVP code 1046) is of type Unsigned 32. The AVP is used for deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations (typically used for admission control of GBR traffic). The AVP can also be used to decide which existing bearers to pre-empt during resource limitations. The priority level defines the relative importance of a resource request.

Values 1 to 15 are defined, with value 1 as the highest level of priority.

Editor"s Note: CT4 has also defined an ARP AVP in TS29.272 which is similar to ARP-Value AVP defined here. It is FFS how to reconcile this.

5.3.46 Pre-emption-Capability AVP (Applicable access type 3GPP-EPS)

The Pre-emption-Capability AVP (AVP code 1047) is of type Enumerated. The AVP defines whether a service data flow can get resources that were already assigned to another service data flow with a lower priority level.

The following values are defined:

PRE-EMPTION_CAPABILITY_ENABLED (0)

This value indicates that the service data flow is allowed to get resources that were already assigned to another service data flow with a lower prioriy level.

PRE-EMPTION_CAPABILITY_DISABLED (1)

This value indicates that the service data flow is not allowed to get resources that were already assigned to another service data flow with a lower prioriy level. This is the default value applicable if this AVP is not supplied.

5.3.47 Pre-emption-Vulnerability AVP (Applicable access type 3GPP-EPS)

The Pre-emption Vulnerability AVP (AVP code 1048) is of type Enumberated. The AVP defines whether a service data flow can lose the resources assigned to it in order to admit a service data flow with higher priority level.

The following values are defined:

PRE-EMPTION_VULNERABILITY_ENABLED (0)

This value indicates that the resources assigned to the service data flow can be pre-empted and allocated to a service data flow with a higher priority level. This is the default value applicable if this AVP is not supplied.

PRE-EMPTION_VULNERABILITY_DISABLED (1)

This value indicates that the resources assigned to the service data flow shall not be pre-empted and allocated to a service data flow with a higher priority level.

5.3.48 Default-EPS-Bearer-QoS AVP

The Default-EPS-Bearer-QoS AVP (AVP code 1049) is of type Grouped, and it defines the QoS information for the EPS default bearer. When this AVP is sent from the PCEF to the PCRF, it indicates the subscribed QoS for the default EPS bearer. When this AVP is sent from the PCRF to the PCEF, it indicates the authorized QoS for the default EPS bearer.

The QoS class identifier identifies a set of IP-CAN specific QoS parameters that define QoS, excluding the applicable bitrates and ARP. When included in the Default-EPS-Bearer-QoS AVP, it shall include only non-GBR values.

The Allocation-Retention-Priority AVP is an indicator of the priority of allocation and retention for the default bearer.

AVP Format:

```
Default-EPS-Bearer-QoS::=   < AVP Header: 1049 >
                            [ QoS-Class-Identifier ]
                            [ Allocation-Retention-Priority]
                          * [AVP]
```

5.3.49 AN-GW-Address AVP (All access types)

The AN-GW-Address AVP (AVP code 1050) is of type Address, and it contains the IPv4 or IPv6 (if available) address(es) of the access node gateway (SGW for 3GPP and AGW for non-3GPP networks).

5.4 Gx re-used AVPs

Table 5.4 lists the Diameter AVPs re-used by the Gx reference point from existing Diameter Applications, reference to their respective specifications, short description of their usage within the Gx reference point and the applicability of the AVPs to charging control, policy control or both. 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 5.4, but they are re-used for the Gx reference point. Where 3GPP Radius VSAs are re-used, they shall be translated to Diameter AVPs as described in RFC 4005 [12] with the exception that the 'M' flag shall be set and the 'P' flag may be set.

Table 5.4: Gx re-used Diameter AVPs

Attribute Name	Reference	Description	Acc. type	Applicablity (note 1)
3GPP-SGSN-Address	3GPP TS 29.061 [11]	For GPRS the IPv4 address of the SGSN	3GPP-GPRS, 3GPP-EPS	Both
3GPP-SGSN-IPv6-Address	3GPP TS 29.061 [11]	For GPRS the IPv6 address of the SGSN	3GPP-GPRS. 3GPP-EPS	Both
3GPP-SGSN-MCC-MNC	3GPP TS 29.061 [11]	For GPRS the MCC and the MNC of the SGSN. For 3GPP/non-3GPP accesses the MCC and the MNC provided by the serving gateway (SGW or AGW). Not applicable for WLAN accesses	All	Both
3GPP-User-Location-Info	3GPP TS 29.061 [11]	For GPRS indicates details of where the UE is currently located (e.g. SAI or CGI)	3GPP-GPRS. 3GPP-EPS	Both
Access-Network-Charging-Address	3GPP TS 29.214 [10]	Indicates the IP Address of the network entity within the access network performing charging (e.g. the GGSN IP address).	All	CC
Access-Network-Charging-Identifier-Value	3GPP TS 29.214 [10]	Contains a charging identifier (e.g. GCID).	All	CC
AF-Charging-Identifier	3GPP TS 29.214 [10]	The AF charging identifier that may be used in charging correlation. For IMS the ICID. This AVP may only be included in a Charging-Rule_Definition AVP if the SERVICE_IDENTIFIER_LEVEL reporting is being selected with the Reporting-Level AVP.	All	CC
Called-Station-ID	IETF RFC 4005 [12]	The address the user is connected to. For GPRS the APN.	All	Both
CC-Request-Number	IETF RFC 4006 [9]	The number of the request for mapping requests and answers	All	Both
CC-Request-Type	IETF RFC 4006 [9]	The type of the request (initial, update, termination)	All	Both
Charging-Information	3GPP TS 29.229 [14]	The Charging-Information AVP is of type Grouped, and contains the addresses of the charging functions in the following AVPs: • Primary-Event-Charging-Function-Name is of type DiameterURI and defines the address of the primary online charging system. The protocol definition in the DiameterURI shall be either omitted or supplied with value "Diameter". • Secondary-Event-Charging-Function-Name is of type DiameterURI and defines the address of the secondary online charging system for the bearer. The protocol definition in the DiameterURI shall be either omitted or supplied with value "Diameter". • Primary-Charging-Collection-Function-Name is of type DiameterURI and defines the address of the primary offline charging system for the bearer. If the GTP' protocol is applied on the Gz interface as specified in 3GPP TS 32.295 [16], the protocol definition in the DiameterURI shall be omitted. If Diameter is applied on the Gz interface, the protocol definition in DiameterURI shall be either omitted or supplied with value "Diameter". The choice of the applied protocol on the Gz interface depends upon configuration in the PCEF. • Secondary-Charging-Collection-Function-Name is of type DiameterURI and defines the address of the secondary offline charging	All	CC

Attribute Name	Reference	Description	Acc. type	Applicablity (note 1)
		system for the bearer. If the GTP' protocol is applied on the Gz interface as specified in 3GPP TS 32.295 [16], the protocol definition in the DiameterURI shall be omitted. If Diameter is applied on the Gz interface, the protocol definition in DiameterURI shall be either omitted or supplied with value "Diameter". The choice of the applied protocol on the Gz interface depends upon configuration in the PCEF.		
Final-Unit-Indication	IETF RFC 4006 [9]	The action applied by the PCEF, and the related filter parameters and redirect address parameters (if available), when the user's account cannot cover the service cost.	All	CC
Flow-Description	3GPP TS 29.214 [10]	Defines the service flow filter parameters for a PCC rule	All	Both
Flows	3GPP TS 29.214 [10]	The flow identifiers of the IP flows related to a PCC rule as provided by the AF. May be only used in charging correlation together with AF-Charging-Identifier AVP.	All	CC
Flow-Status	3GPP TS 29.214 [10]	Defines whether the service flow is enabled or disabled. The value "REMOVED" is not applicable to Gx.	All	Both
Framed-IP-Address	IETF RFC 4005 [12]	The IPv4 address allocated for the user.	All	Both
Framed-IPv6-Prefix	IETF RFC 4005 [12]	The IPv6 address prefix allocated for the user. The encoding of the value within this Octet String type AVP shall be as defined in IETF RFC 3162 [15], Clause 2.3. The "Reserved", "Prefix-Length" and "Prefix" fields shall be included in this order.	All	Both
Max-Requested-Bandwidth-UL (note 2)	3GPP TS 29.214 [10]	Defines the maximum authorized bandwidth for uplink.	All	PC
Max-Requested-Bandwidth-DL (note 2)	3GPP TS 29.214 [10]	Defines the maximum authorized bandwidth for downlink.	All	PC
RAI	3GPP TS 29.061 [11]	Contains the Routing Area Identity of the SGSN where the UE is registered	3GPP-GPRS. 3GPP-EPS	Both
Rating-Group	IETF RFC 4006 [9]	The charging key for the PCC rule used for rating purposes	All	CC
Service-Identifier	IETF RFC 4006 [9]	The identity of the service or service component the service data flow in a PCC rule relates to.	All	CC
Subscription-Id	IETF RFC 4006 [9]	The identification of the subscription (IMSI, MSISDN, etc)	All	Both
User-Equipment-Info	IETF RFC 4006 [9]	The identification and capabilities of the terminal (IMEISV, etc.) When the User-Equipment-Info-Type is set to IMEISV(0), the value within the User-Equipment-Info-Value shall be a UTF-8 encoded decimal.	All	Both
3GPP-MS-TimeZone	3GPP TS 29.061 [11]	Indicate the offset between universal time and local time in steps of 15 minutes of where the MS currently resides.	All	Both

NOTE 1: AVPs marked with 'CC' are applicable to charging control, AVPs marked with 'PC' are applicable to policy control and AVPs marked with 'Both' are applicable to both charging control and policy control.
NOTE 2: When sending from the PCRF to the PCEF, the Max-Requested-Bandwidth-UL/DL AVP indicate the maximum allowed bit rate for the uplink/downlink direction; when sending from the PCEF to the PCRF, the Max-Requested-Bandwidth-UL/DL AVP indicate the maximum requested bit rate for the uplink/downlink direction.

5.5 Gx specific Experimental-Result-Code AVP values

5.5.1 General

RFC 3588 [5] specifies the Experimental-Result AVP containing Vendor-ID AVP and 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 a request. The Vendor-ID AVP shall be set to 3GPP (10415).

5.5.2 Success

Result Codes that fall within the Success category are used to inform a peer that a request has been successfully completed.

The Result-Code AVP values defined in Diameter BASE RFC 3588 [5] shall be applied.

5.5.3 Permanent Failures

Errors that fall within the Permanent Failures category shall be used to inform the peer that the request failed, and should not be attempted again.

The Result-Code AVP values defined in Diameter BASE RFC 3588 [5] are applicable. Also the following specific Gx Experimental-Result-Codes values are defined:

DIAMETER_ERROR_INITIAL_PARAMETERS (5140)

This error shall be used when the set of bearer or session or subscriber information needed by the PCRF for rule selection is incomplete or erroneous or not available for the decision to be made. (e.g. QoS, SGSN address, RAT type, TFT, subscriber information)

DIAMETER_ERROR_TRIGGER_EVENT (5141)

This error shall be used when the set of bearer/session information sent in a CCR originated due to a trigger event been met is incoherent with the previous set of bearer/session information for the same bearer/session. (e.g event trigger met was RAT changed, and the RAT notified is the same as before)

DIAMETER_PCC_RULE_EVENT (5142)

This error shall be used when the PCC rules cannot be installed/activated. Affected PCC-Rules will be provided in the Charging-Rule-Report AVP including the reason and status as described in Clause 4.5.12. Absence of the Charging-Rule-Report means that all provided PCC rules for that specific bearer/session are affected.

DIAMETER_ERROR_BEARER_NOT_AUTHORIZED (5143)

This error shall be used when the PCRF cannot authorize an IP-CAN bearer (e.g. the authorized QoS would exceed the subscribed QoS) upon the reception of an IP-CAN bearer authorization request coming from the PCEF. The affected IP-CAN bearer is the one that triggered the corresponding CCR. The PCEF shall reject the attempt to initiate or modify the bearer indicated in the related CCR command.

DIAMETER_ERROR_TRAFFIC_MAPPING_INFO_REJECTED (5144)

This error shall be used when the PCRF does not accept one or more of the traffic mapping filters (e.g. TFT filters for GPRS) provided by the PCEF in a CC Request.

5.5.4 Transient Failures

Errors that fall within the transient failures category are used to inform a peer that the request could not be satisfied at the time it was received, but may be able to satisfy the request in the future.

The Result-Code AVP values defined in Diameter Base RFC 3588 [5] are applicable. Also the following specific Gx Experimental-Result-Code value is defined for transient failures:

DIAMETER_PCC_BEARER_EVENT (4141)

This error shall be used when for some reason a PCC rule cannot be enforced or modified successfully in a network initiated procedure. Affected PCC-Rules will be provided in the Charging-Rule-Report AVP including the reason and status as described in Clause 4.5.12.

5.6 Gx Messages

5.6.1 Gx Application

Gx Messages are carried within the Diameter Application(s) described in clause 5.1.

Existing Diameter command codes from the Diameter base protocol RFC 3588 [5] and the Diameter Credit Control Application RFC 4006 [9] are used with the Gx specific AVPs specified in clause 5.3. The Diameter Credit Control Application AVPs and AVPs from other Diameter applications that are re-used are defined in clause 5.4. Due to the definition of these commands there is no possibility to skip the Auth-Application-Id AVP and use the Vendor-Specific-Application-Id AVP instead. Therefore the Gx application identifier shall be included in the Auth-Application-Id AVP.

In order to support both PULL and PUSH procedures, a diameter session needs to be established for each IP-CAN session. For IP-CAN types that support multiple IP-CAN bearers (as in the case of GPRS), the diameter session is established when the very first IP-CAN bearer for the IP-CAN session is established.

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 message definition in the DCC Application RFC 4006 [9] or Diameter Base Protocol RFC 3588 [5].

5.6.2 CC-Request (CCR) Command

The CCR command, indicated by the Command-Code field set to 272 and the 'R' bit set in the Command Flags field, is sent by the PCEF to the PCRF in order to request PCC rules for a bearer. The CCR command is also sent by the PCEF to the PCRF in order to indicate bearer or PCC rule related events or the termination of the IP CAN bearer and/or session.

Message Format:

```
<CC-Request> ::= < Diameter Header: 272, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { CC-Request-Type }
                 { CC-Request-Number }
                 [ Destination-Host ]
                 [ Origin-State-Id ]
                *[ Subscription-Id ]
                 [ Network-Request-Support ]
                 [ Bearer-Identifier ]
                 [ Bearer-Operation ]
                 [ Framed-IP-Address ]
                 [ Framed-IPv6-Prefix ]
                 [ IP-CAN-Type ]
                 [RAT-Type ]
                 [ Termination-Cause ]
                 [ User-Equipment-Info ]
                 [ QoS-Information ]
                 [ QoS-Negotiation ]
                 [ QoS-Upgrade ]
                 [ Default-EPS-Bearer-QoS ]
                *[ AN-GW-Address ]
                 [ 3GPP-SGSN-MCC-MNC ]
                 [ 3GPP-SGSN-Address ]
                 [ 3GPP-SGSN-IPv6-Address ]
                 [ RAI ]
                 [ 3GPP-User-Location-Info]
                    [ 3GPP-MS-TimeZone ]
                 [ Called-Station-ID ]
                 [ Bearer-Usage ]
                 [ Online ]
                 [ Offline ]
```

```
                *[ TFT-Packet-Filter-Information ]
                *[ Charging-Rule-Report]
                *[ Event-Trigger]
                 [ Event-Report-Indication]
                 [ Access-Network-Charging-Address ]
                *[ Access-Network-Charging-Identifier-Gx ]
                *[ CoA-Information ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

5.6.3 CC-Answer (CCA) Command

The CCA command, indicated by the Command-Code field set to 272 and the 'R' bit cleared in the Command Flags field, is sent by the PCRF to the PCEF in response to the CCR command. It is used to provision PCC rules and event triggers for the bearer/session and to provide the selected bearer control mode for the IP-CAN session. If the PCRF performs the bearer binding, PCC rules will be provisioned at bearer level. The primary and secondary CCF and/or primary and secondary OCS addresses may be included in the initial provisioning.

Message Format:

```
<CC-Answer> ::=  < Diameter Header: 272, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 { CC-Request-Type }
                 { CC-Request-Number }
                 [ Bearer-Control-Mode ]
                *[ Event-Trigger ]
                 [ Origin-State-Id ]
                *[ Charging-Rule-Remove ]
                *[ Charging-Rule-Install ]
                 [ Charging-Information ]
                 [ Online ]
                 [ Offline ]
                *[ QoS-Information ]
                 [ Revalidation-Time ]
                 [ Default-EPS-Bearer-QoS ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

5.6.4 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 BBERF/PCEF in order to provision QoS/PCC rules using the PUSH procedure initiate the provision of unsolicited QoS/PCC rules. It is used to provision QoS/PCC rules, event triggers and event report indications for the session. If the PCRF performs the bearer binding, PCC rules will be provisioned at bearer level.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Re-Auth-Request-Type }
                 [ Session-Release-Cause ]
                 [ Origin-State-Id ]
                *[ Event-Trigger ]
                 [ Event-Report-Indication ]
                *[ Charging-Rule-Remove ]
                *[ Charging-Rule-Install ]
                 [ Default-EPS-Bearer-QoS ]
                *[ QoS-Information ]
```

```
                [ Revalidation-Time ]
               *[ Proxy-Info ]
               *[ Route-Record ]
               *[ AVP]
```

5.6.5 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 PCEF 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 ]
                 [ Origin-State-Id ]
                *[ Charging-Rule-Report]
                 [ Access-Network-Charging-Address ]
                *[ Access-Network-Charging-Identifier-Gx ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ AVP ]
```

5a Gxx protocols

Editor's note: The structure of this clause may change

5a.1 Protocol support

The Gxx application is defined as a vendor specific Diameter application, where the vendor is 3GPP and the Application-ID for the Gxx Application in the present release is xxx. The vendor identifier assigned by IANA to 3GPP (http://www.iana.org/assignments/enterprise-numbers) is 10415.

Editor"s Note: A new Diameter application-id is required for Gxx from IANA

NOTE: A route entry can have a different destination based on the application identification AVP of the message. Therefore, Diameter agents (relay, proxy, redirection, translation agents) must be configured appropriately to identify the 3GPP Gxx application within the Auth-Application-Id AVP in order to create suitable routeing tables.

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

With regard to the Diameter protocol defined over the Gxx interface, the PCRF acts as a Diameter server, in the sense that it is the network element that handles QoS Rule requests for a particular realm. The BBERF acts as the Diameter client, in the sense that it is the network element requesting QoS rules in the transport plane network resources.

5a.2 Initialization, maintenance and termination of connection and session

The initialization and maintenance of the connection between the BBERF and PCRF (visited or home) are defined by the underlying protocol. Establishment and maintenance of connections between Diameter nodes are described in IETF RFC 3588 [5].

After establishing the transport connection, the PCRF and the BBERF shall advertise the support of the Gxx specific Application by including the value of the application identifier in the Auth-Application-Id AVP and the value of the

3GPP (10415) in the Vendor-Id AVP of the Vendor-Specific-Application-Id AVP contained in the Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands. The Capabilities-Exchange-Request and Capabilities-Exchange-Answer commands are specified in the Diameter Base Protocol (RFC 3588 [5]).

The termination of the Diameter user session is specified in RFC 3588 [5] in clauses 8.4 and 8.5. The description of how to use of these termination procedures in the normal cases is embedded in the procedures description.

5a.3 Gxx specific AVPs

Table 5a.3.1 describes the Diameter AVPs defined for the Gxx reference point, their AVP Code values, types, possible flag values, whether or not the AVP may be encrypted and what access types (e.g. 3GPP-GPRS, etc.) the AVP is applicable to. The Vendor-Id header of all AVPs defined in the present document shall be set to 3GPP (10415).

Table 5a.3.1: Gxx specific Diameter AVPs

Attribute Name	AVP Code	Clause defined	Value Type (note 2)	AVP Flag rules (note 1)				May Encr.	Acc. type
				Must	May	Should not	Must not		
QoS-Rule-Install	1051	5a.3.1	Grouped	M,V	P			Y	All
QoS-Rule-Remove	1052	5a.3.2	Grouped	M,V	P			Y	All
QoS-Rule-Definition	1053	5a.3.3	Grouped	M,V	P			Y	All
QoS-Rule-Name	1054	5a.3.4	OctetString	M,V	P			Y	All
QoS-Rule-Report	1055	5a.3.5	Grouped	M,V	P			Y	All

Editor"s Note: It is FFS if the 3GPP-SGSN-MCC-MNC AVP is reused or a new one is defined with a generic name (e.g. AN-MCC-MNC)

5a.3.1 QoS-Rule-Install AVP (All access types)

The QoS-Rule-Install AVP (AVP code 1051) is of type Grouped, and it is used to activate, install or modify QoS rules as instructed from the PCRF to the BBERF.

For installing a new QoS rule or modifying a QoS rule already installed, QoS-Rule-Definition AVP shall be used.

When Tunnel-Information AVP is provided it applies to all the QoS rules included within the QoS-Rule-Install AVP. For QoS rules are being modified, the newly provided Tunnel-Information AVP replaces previously provided Tunnel-Information AVP for the modified QoS rules.

AVP Format:

```
QoS-Rule-Install ::= < AVP Header: 1051>
                            *[ QoS-Rule-Definition ]
                             [ Tunnel-Information ]
                            *[ AVP ]
```

5a.3.2 QoS-Rule-Remove AVP (All access types)

The QoS-Rule-Remove AVP (AVP code 1052) is of type Grouped, and it is used to deactivate or remove QoS rules from an Gateway Control session.

QoS-Rule-Name AVP is a reference for a specific QoS rule at the BBERF to be removed.AVP Format:

```
QoS-Rule-Remove ::= < AVP Header: 1052>
                            *[ QoS-Rule-Name ]
                            *[ AVP ]
```

5a.3.3 QoS-Rule-Definition AVP (All access types)

The QoS-Rule-Definition AVP (AVP code 1053) is of type Grouped, and it defines the QoS rule for a service flow sent by the PCRF to the BBERF. The QoS-Rule-Name AVP uniquely identifies the QoS rule and it is used to reference to a QoS rule in communication between the BBERF and the PCRF within one Gateway Control session. The Flow-Description AVP(s) determines the traffic that belongs to the service flow.

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

AVP Format:

```
QoS-Rule-Definition ::= < AVP Header: 1053>
                          { QoS-Rule-Name }
                         *[ Flow-Description ]
                          [ QoS-Information ]
                          [ Precedence ]
                         *[ AVP ]
```

5a.3.4 QoS-Rule-Name AVP (All access types)

The QoS-Rule-Name AVP (AVP code 1054) is of type OctetString, and it defines a name for QoS rule. For QoS rules provided by the PCRF it uniquely identifies a QoS rule within one Gateway Control session.

5a.3.5 QoS-Rule-Report AVP (All access types)

The QoS-Rule-Report AVP (AVP code 1055) is of type Grouped, and it is used to report the status of QoS rules.

QoS-Rule-Name AVP is a reference for a specific QoS rule at the BBERF that has been successfully installed, modified or removed.

The QoS-Rule-Report AVP can also be used to report the status of the QoS rules which cannot be installed or enforced at the BBERF. In this condition, the QoS-Rule-Name AVP is used to indicate a specific QoS rule which cannot be installed or enforced. The Rule-Failure-Code AVP indicates the reason that the QoS rules cannot be successfully installed or enforced.

AVP Format:

```
QoS-Rule-Report ::= < AVP Header: 1055>
                      *[ QoS-Rule-Name ]
                       [ PCC-Rule-Status ]
                       [ Rule-Failure-Code ]
                      *[ AVP ]
```

Multiple instances of QoS-Rule-Report AVPs shall be used in the case it is required to report different PCC-Rule-Status or Rule-Failure-Code values for different rules within the same Diameter command.

5a.4 Gxx re-used AVPs

Table 5a.4.1 lists the Diameter AVPs re-used by the Gxx reference point from Gx reference point and other existing Diameter Applications, reference to their respective specifications, short description of their usage within the Gxx reference point and the applicability of the AVPs to a specific access. When reused from Gx reference point, the specific clause in the present specification is referred. 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 5a.4, but they are re-used for the Gxx reference point. Where RADIUS VSAs are re-used, they shall be translated to Diameter AVPs as described in RFC 4005 [12] with the exception that the 'M' flag shall be set and the 'P' flag may be set.

Table 5a.4.1: Gxx re-used Diameter AVPs

Attribute Name	Reference	Description	Acc. type
3GPP-SGSN-Address	3GPP TS 29.061 [11]	For GPRS the IPv4 address of the SGSN	3GPP-GPRS 3GPP-EPS
3GPP-SGSN-IPv6-Address	3GPP TS 29.061 [11]	For GPRS the IPv6 address of the SGSN	3GPP-GPRS 3GPP-EPS
3GPP-User-Location-Info	3GPP TS 29.061 [11]	Indicates details of where the UE is currently located (e.g. SAI or CGI)	3GPP-GPRS 3GPP-EPS
3GPP2-BSID	3GPP2 X.S0011-D [20]	For 3GPP2 indicates the BSID of where the UE is currently located (e.g. Cell-Id, SID, NID). The Vendor-Id shall be set to 3GPP2 (5535) [20]. The support of this AVP shall be advertised in the capabilities exchange mechanisms (CER/CEA) by including the value 5535, identifying 3GPP2, in a Supported-Vendor-Id AVP.	3GPP2
Allocation-and-Retention-Priority	5.3.32	Indicates a priority for accepting or rejecting a bearer establishment or modification request and dropping a bearer in case of resource limitations.	All
APN-Aggregate-Max-Bitrate-DL	5.3.39	Indicates the aggregate maximum bitrate for the downlink direction for all non-GBR bearers of the APN.	3GPP-EPS
APN-Aggregate-Max-Bitrate-UL	5.3.40	Indicates the aggregate maximum bitrate for the uplink direction for all non-GBR bearers of the APN.	3GPP-EPS
Bearer-Control-Mode	5.3.23	Indicates the PCRF selected bearer control mode.	FFS
Called-Station-ID	IETF RFC 4005 [12]	The address the user is connected to (i.e. the PDN identifier).	All
CC-Request-Number	IETF RFC 4006 [9]	The number of the request for mapping requests and answers	All
CC-Request-Type	IETF RFC 4006 [9]	The type of the request (initial, update, termination)	All
Event-Trigger	5.3.7	Reports the event that occurred on the BBERF. For Event-Trigger LOSS_OF_BEARER, BBERF will include the impacted QoS rules within the QoS-Rule-Report. For Event-Trigger RECOVERY_OF_BEARER BBERF will include the impacted QoS rules within the QoS-Rule-Report. For 3GPP2 access USER_LOCATION_CHANGE is used to report and request changes to the 3GPP2-BSID. The following values are not applicable: PLMN_CHANGE (4), IP-CAN_CHANGE (7), QOS_EXCEEDING_AUTHORIZATION (11), OUT_OF_CREDIT (15), REALLOCATION_OF_CREDIT (16), IP_ADDRESS_ALLOCATE (18) and IP_ADDRESS_RELEASE (19).	All
Flow-Description	3GPP TS 29.214 [10]	Defines the service flow filter parameters for a QoS rule	All
Framed-IP-Address	IETF RFC 4005 [12]	The IPv4 address allocated for the user.	All
Framed-IPv6-Prefix	IETF RFC 4005 [12]	The IPv6 address prefix allocated for the user. The encoding of the value within this Octet String type AVP shall be as defined in IETF RFC 3162 [15], Clause 2.3. The 'Reserved', 'Prefix-Length' and 'Prefix' fields shall be included in this order.	All
Guaranteed-Bitrate-DL (note 1)	5.3.25	Defines the guaranteed bitrate for downlink.	All
Guaranteed-Bitrate-UL (note 1)	5.3.26	Defines the guaranteed bitrate for uplink.	All
IP-CAN-Type	5.3.27	Indicates the type of Connectivity Access Network that the user is connected to.	All
Max-Requested-Bandwidth-UL (note 2)	3GPP TS 29.214 [10]	Defines the maximum authorized bandwidth for uplink.	All
Max-Requested-Bandwidth-DL (note 2)	3GPP TS 29.214 [10]	Defines the maximum authorized bandwidth for downlink.	All

Attribute Name	Reference	Description	Acc. type
Network-Request-Support	5.3.24	Indicates whether the access network supports the network requested bearer control mode or not.	All
Precedence	5.3.11	Indicates the precedence of QoS rules or packet filters.	All
PCC-Rule-Status	5.3.19	Describes the status of one or a group of QoS rules.	All
QoS-Class-Identifier	5.3.17	Identifies a set of IP-CAN specific QoS parameters	All
QoS-Information	5.3.16	. Defines the QoS information for a resource, QoS rule or QCI	All
Default-EPS-Bearer-QoS	5.3.48	Defines the QoS information of the default bearer	All (See NOTE 3)
RAI	3GPP TS 29.061 [11]	Contains the Routing Area Identity of the SGSN where the UE is registered	3GPP-GPRS 3GPP-EPS
RAT-Type	5.3.31	Identifies the radio access technology that is serving the UE.	All
Rule-Failure-Code	5.3.38	Identifies the reason a QoS rule is being reported.	All
Session-Release-Cause	5.3.44	Indicate the reason of termination initiated by the PCRF. Only the reason code UNSPECIFIED_REASON is applicable for the PCRF-initiated Gxx session termination.	All
Subscription-Id	IETF RFC 4006 [9]	The identification of the subscription (i.e.IMSI)	All
TFT-Filter	5.3.13	FFS	All
TFT-Packet-Filter-Information	5.3.14	FFS	All
ToS-Traffic-Class	5.3.15	FFS	All
Tunnel-Header-Filter	5.3.34	Defines the tunnel (outer) header filter information of a tunnelled IP flow.	Non-3GPP
Tunnel-Header-Length	5.3.35	Indicates the length of the tunnel (outer) header.	Non-3GPP
Tunnel-Information	5.3.36	Defines the tunnel (outer) header information for an IP flow.	Non-3GPP
User-Equipment-Info	IETF RFC 4006 [9]	The identification and capabilities of the terminal (IMEISV, etc.) When the User-Equipment-Info-Type is set to IMEISV(0), the value within the User-Equipment-Info-Value shall be a UTF-8 encoded decimal.	All

NOTE 1: When sending from the PCRF to the BBERF, the Guaranteed-Bitrate-UL/DL AVP indicate the allowed guaranteed bit rate for the uplink/downlink direction; when sending from the BBERF to the PCRF, the Guaranteed-Bitrate-UL/DL AVP indicate the requested guaranteed bit rate for the uplink/downlink direction.
NOTE 2: When sending from the PCRF to the BBERF, the Max-Requested-Bandwidth-UL/DL AVP indicate the maximum allowed bit rate for the uplink/downlink direction; when sending from the BBERF to the PCRF, the Max-Requested-Bandwidth-UL/DL AVP indicate the maximum requested bit rate for the uplink/downlink direction.
NOTE 3: Default-EPS-Bearer-QoS does not apply for 3GPP-GPRS access type.

Editor"s Note: It is FFS whether Bearer-Identifier and Bearer-Usage AVPs as defined in Gx Rel-7 can be reused for resource handling and default bearer handling, or whether specific AVPs are required. It is also FFS the applicability of these AVPs for 3GPP 2G/3G accesses and non-3GPP accesses.

Editor"s Note: An AVP that indicates resource initiation, modification or termination is required. It is FFS if Bearer-Operation AVP can be used for that purpose.

Editor"s Note: 3GPP-SGSN-Address and 3GPP-SGSN-IPv6-Address, are used to convey the related SGSN information when SGSN is connected to SGW via S4. It is FFS what AVPs are used to convey the SGW/AGW address.

Editor"s Note: TFT-Filter, TFT-Packet-Filter-Information and ToS-Traffic-Class are currently defined in the context of GPRS. It is FFS what they mean in the context of Gxx for both 3GPP and non-3GPP accesses.

Editor"s Note: It is FFS if the 3GPP-SGSN-MCC-MNC AVP is reused or a new one is defined with a generic name (e.g. AN-MCC-MNC)

Editor"s Note: It is FFS if PDN id can be considered for Gxx application.

5a.5 Gxx specific Experimental-Result-Code AVP values

The same codes specified in clause 5.5 apply here with the following exceptions:

The following permanent Experimental-Result-Code shall be used instead of DIAMETER_PCC_RULE_EVENT (5142):

DIAMETER_QOS_RULE_EVENT (5145)

This error shall be used when the QoS rules cannot be installed/activated. Affected QoS-Rules will be provided in the QoS-Rule-Report AVP including the reason and status as described in Clause 4a.5.5.

The following transient Experimental-Result-Code shall be used instead of DIAMETER_PCC_BEARER_EVENT (4141):

DIAMETER_BEARER_EVENT (5146)

This error shall be used when for some reason a QoS rule cannot be enforced or modified successfully in a network initiated procedure. Affected QoS Rules will be provided in the QoS-Rule-Report AVP including the reason and status as described in Clause 4a.5.5.

5a.6 Gxx Messages

5a.6.1 Gxx Application

Gxx Messages are carried within the Diameter Application(s) described in clause 5a.1.

Existing Diameter command codes from the Diameter base protocol RFC 3588 [5] and the Diameter Credit Control Application RFC 4006 [9] are used with the Gxx specific AVPs specified in clause 5a.3. The Diameter Credit Control Application AVPs and AVPs from other Diameter applications that are re-used are defined in clause 5a.4. Due to the definition of these commands there is no possibility to skip the Auth-Application-Id AVP and use the Vendor-Specific-Application-Id AVP instead. Therefore the Gxx application identifier shall be included in the Auth-Application-Id AVP. A diameter session needs to be established for each Gateway Control session.

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 message definition in the DCC Application RFC 4006 [9] or Diameter Base Protocol RFC 3588 [5].

5a.6.2 CC-Request (CCR) Command

The CCR command, indicated by the Command-Code field set to 272 and the 'R' bit set in the Command Flags field, is sent by the BBERF to the PCRF in order to request QoS rules. The CCR command is also sent by the BBERF to the PCRF in order to indicate QoS rule related events or the termination of the Gateway Control session.

Message Format:

```
<CC-Request> ::= < Diameter Header: 272, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { CC-Request-Type }
                 { CC-Request-Number }
                 [ Destination-Host ]
                 [ Origin-State-Id ]
                *[ Subscription-Id ]
                 [ Network-Request-Support ]
                 [ Framed-IP-Address ]
                 [ Framed-IPv6-Prefix ]
                 [ IP-CAN-Type ]
                 [ RAT-Type ]
                 [ User-Equipment-Info ]
                 [ QoS-Information ]
                 [ Default-EPS-Bearer-QoS ]
                 [ QoS-Negotiation ]
```

```
                  [ 3GPP-SGSN-Address ]
                  [ 3GPP-SGSN-IPv6-Address ]
                  [ RAI ]
                  [ 3GPP-User-Location-Info]
                  [ 3GPP2-BSID ]
                  [ Called-Station-ID ]
                 *[ TFT-Packet-Filter-Information ]
                 *[ QoS-Rule-Report]
                 *[ Event-Trigger]
                 *[ Proxy-Info ]
                 *[ Route-Record ]
                 *[ AVP ]
```

Editor"s Note: It is FFS which AVP will be used to convey UE resource request related information.

5a.6.3 CC-Answer (CCA) Command

The CCA command, indicated by the Command-Code field set to 272 and the 'R' bit cleared in the Command Flags field, is sent by the PCRF to the BBERF in response to the CCR command. It is used to provision QoS rules and event triggers for the bearer/session and to provide the selected bearer control mode for the Gateway Control session.

Message Format:

```
<CC-Answer> ::=  < Diameter Header: 272, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                 { CC-Request-Type }
                 { CC-Request-Number }
                 [ Bearer-Control-Mode ]
                *[ Event-Trigger ]
                 [ Origin-State-Id ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ QoS-Rule-Remove ]
                *[ QoS-Rule-Install ]
                *[ QoS-Information ]
                 [ Default-EPS-Bearer-QoS ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ Route-Record ]
                *[ AVP ]
```

5a.6.4 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 BBERF in order to provision QoS rules using the PUSH procedure initiate the provision of unsolicited QoS rules. It is used to provision QoS rules, event triggers and event report indications for the session.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Re-Auth-Request-Type }
                 [ Session-Release-Cause ]
                 [ Origin-State-Id ]
                *[ Event-Trigger ]
                *[ QoS-Rule-Remove ]
                *[ QoS-Rule-Install ]
                *[ QoS-Information ]
                 [ Default-EPS-Bearer-QoS ]
                *[ Proxy-Info ]
                *[ Route-Record ]
```

```
                *[ AVP]
```

5a.6.5 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 BBERF 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 ]
                 [ Origin-State-Id ]
                *[ QoS-Rule-Report]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                *[ Proxy-Info ]
                *[ AVP ]
```

Annex A (normative): Access specific aspects (GPRS)

A.1 Scope

This annex defines access specific aspects procedures for use of Gx/Gxx between PCRF and a GPRS IP-CAN.

A.2 Reference Model

In GPRS IP-CAN, the BBERF does not apply. The Gxx reference point is not applicable.

A.2 Functional Elements

A.2.1 PCRF

For GPRS it shall be possible to support policy control, i.e. access control and QoS control, on a per-PDP context basis for the UE initiated bearer control case.

A.3 PCC procedures

A.3.1 Request for PCC rules

At IP-CAN session establishment as described in clause 4.5.1, information about the user equipment (e.g. IMEISV), QoS negotiated and further QoS related information as detailed in Clause A.3.3.1, user location information (e.g. RAI, CGI/SAI) SGSN Address, SGSN country and network codes, APN, TFT and indication if the bearer is used as IMS signalling PDP context shall be provided. The PCEF shall provide the Bearer-Identifier AVP at the IP-CAN session establishment. In this case, the PCEF shall also include the Bearer-Operation AVP set to the value "Establishment".

IP-CAN session modification with PCEF-requested rules, as described in clause 4.5.1, can occur in the following cases:

- When a new PDP Context is being established by the UE in an already existing IP-CAN Session.
- When a PDP context is being modified and an Event trigger is met.
- When a PDP context is being terminated.

If the PCRF does not accept one or more of the TFT filters provided by the PCEF in a CC Request (e.g. because the PCRF does not allow the UE to request enhanced QoS for services not known to the PCRF), the PCRF shall reject the request using a CC Answer with the Gx experimental result code TRAFFIC_MAPPING_INFO_REJECTED (5144). If the PCEF receives a CC Answer with this code, the PCEF shall reject the IP-CAN session establishment or modification that initiated the CC Request by applying a proper cause code and other parameters as per 3GPP TS 29.060 [18].

A.3.2 Provisioning of PCC rules

A.3.2.2 Selecting a PCC rule and IP CAN Bearer for Downlink IP packets

TFT filters shall not be applied to assign downlink IP packets to PDP contexts if PCC is enabled for an APN.

A.3.3 Provisioning and Policy Enforcement of Authorized QoS

For 3GPP-GPRS, default EPS bearer QoS provisioning and enforcement is not applicable.

A.3.3.1 Provisioning of authorized QoS per IP CAN bearer

As described in clause 4.5.5.0a, the authorized QoS per IP-CAN bearer is used if the bearer binding is performed by the PCRF (as defined in [8]).

When the PCEF request a new PCC decisions using a CCR command including the requested QoS information within the QoS-Information AVP, the PCEF shall use Table A.4.1.1 to map the requested QoS within the IP CAN bearer establishment request to the QoS-Information AVP. If the GGSN receives the 'upgrade QoS Supported' flag set to '1' in the Common Flag Information element within the corresponding Create PDP context request (3GPP TS 29.060[18]), the GGSN shall supply the QoS-Upgrade AVP with value QoS_UPGRADE_SUPPORTED.

If at any point of time the PCEF receives a request for a modification of an already existing IP-CAN bearer that matches event triggers supplied by the PCRF for the IP CAN session, the PCEF shall also request a new PCC decisions using a CCR command including the corresponding event triggers in the Event-Trigger AVP. If a QoS change for the existing IP-CAN bearer is requested the PCEF shall include the requested QoS information within the QoS-Information AVP in the CCR. The PCEF shall use Table A.4.1.1 to map the requested QoS within the IP CAN bearer modification request to the QoS-Information AVP. If the GGSN receives within the corresponding Update PDP context request the 'upgrade QoS Supported' flag in the Common Flag Information element (3GPP TS 29.060[18]) set to a different value than previously communicated to the PCRF, the GGSN shall supply the QoS-Upgrade AVP indicating the new value. If the GGSN receives within the Update PDP context request the 'No QoS negotiation' flag set to '1' in the Common Flag Information element (3GPP TS 29.060[18]), the GGSN shall supply the QoS-Negotiation AVP with the value NO_QoS_NEGOTIATION.

When receiving a CCR with a QoS-Information AVP, the PCRF shall decide upon the requested QoS information within the CCR command. For GPRS, the following restrictions apply to the PCRF QoS authorization process:

- If the QoS-Negotiation AVP is received by the PCRF indicating that QoS negotiation is not allowed, the PCRF shall provision the requested QoS as authorized QoS.

- If the QoS-Upgrade AVP has been received by the PCRF indicating that QoS upgrade is not supported, the PCRF shall not provision an authorized QoS that is higher than the requested QoS.

A.3.3.2 Policy enforcement for authorized QoS per IP CAN bearer

The PCEF is responsible for enforcing the policy based authorization, i.e., to ensure that the requested QoS is in-line with the 'Authorized QoS' per IP-CAN bearer, as described in Clause 4.5.5.1.

Upon reception of an authorized QoS per IP-CAN bearer within a CCA or RAR command, the PCEF shall perform the mapping from that "Authorised QoS" information for the IP-CAN bearer into authorised UMTS QoS information according to Table A.4.1.1. The authorised UMTS QoS information is futher processed by the UMTS BS Manager within the GGSN.

A.3.3.3 Policy enforcement for authorized QoS per service data flow

The mapping from the authorized QoS parameters to the UMTS QoS parameters shall be performed according to Table A.4.1.1.

A.3.3.4 Policy enforcement for authorized QoS per QCI

The mapping from the authorized QoS parameters to the UMTS QoS parameters shall be performed according to Table A.4.1.1.

A.3.4 Indication of IP-CAN Bearer Termination Implications

When a PDP context is terminated, , the PCEF shall apply the "Indication of IP CAN Bearer Termination Implications" procedure to inform the PCRF about implications of this bearer termination if any of the following conditions apply while the IP-CAN Session remains active:

- A PDP Context is terminated, which has been initiated by the UE.

- A PDP Context is terminated, which has been initiated by the network (e.g. SGSN).

Editor's Note: It is ffs if the indication of bearer termination is also applicable if the provisioned total QoS is reduced compared to what has been provisioned in the Authorized-QoS AVP on session level.

The following exceptions to clause 4.5.6 shall apply in 3GPP-GPRS.

When the PCRF performs bearer binding, the PCEF shall also supply the Bearer-Identifier and Bearer-Operation AVPs to indicate "Termination" of a specific bearer in a CC-Request with CC-Request-Type AVP set to the value "UPDATE_REQUEST".

When the PCRF receives the CC-Request indicating the implications of a bearer termination, it shall acknowledge the message by sending a CC-Answer to the PCEF. The PCRF has the option to make a new PCC decision for the affected PCC Rules. Within the CC-answer, the PCRF may provision PCC rules as detailed in clause 4.5.2. When the PCRF performs the bearer binding, the PCRF may provision PCC rules e.g. to move PCC rules previously applied to the terminated IP CAN bearer to any of the remaining IP CAN bearer(s). The Bearer-Identifier of the selected bearer(s) will be provided. The PCEF shall remove all PCC rules previously applied to the terminated IP CAN bearer, which have not been moved.

The PCEF shall remove all PCC rules previously applied to the terminated IP CAN bearer, which have not been moved.

If the last PDP context within an IP CAN session is being terminated, the PCEF shall apply the procedures in clause A.3.5 to indicate the IP CAN session termination

A.3.5 Indication of IP-CAN Session Termination

For GPRS, an IP-CAN session is terminated when the last PDP Context within the IP-CAN session is being terminated. The procedure described in clause 4.5.7 applies here.

A.3.6 Request of IP-CAN Bearer Termination

If no more PCC rules are applied to an IP CAN bearer, the PCEF shall send a PDP context deactivation request.

If the termination of the last IP CAN bearer within an IP CAN session is requested, the PCRF and PCEF shall apply the procedures in clause A.3.7.

If the selected Bearer Control Mode is UE-only, the PCRF may request the termination of an existing IP CAN bearer within an IP CAN session by using the PCC rule provisioning procedures in clause 4.5.2 to remove all PCRF-provisioned PCC rules and deactivate all PCC rules predefined within the PCEF, which have been applied to this IP CAN bearer. The PCRF may either completely remove these PCC rules from the IP CAN session or move them to another IP CAN bearer within the IP CAN session.

If the PCEF performs the IP CAN bearer binding, the PCRF is not aware that it requests the termination of an IP CAN bearer by removing certain PCC rules. If upon removal of the PCC rules, there are no more PCC rules active in the PCEF for an IP-CAN bearer, the PCEF shall initiate the bearer termination procedure. Further details of the binding mechanism can be found in 3GPP TS 29.213 [8].

If the selected Bearer Control Mode (BCM) is UE-only, and the PCRF receives a trigger for the removal of all PCC rules bound to an IP CAN bearer from the AF, the following steps apply. In order to avoid race conditions, the PCRF should start a timer to wait for the UE-initiated termination message. If a UE-initiated termination of an IP CAN bearer is performed before timer expiry, the PCRF will receive an Indication of IP-CAN Bearer Termination Implications according to Clause 4.5.6 and shall then not perform the network-initiated termination of that IP CAN bearer. Otherwise, if the timer expires, the PCRF shall remove/deactivate all the PCC rules that have been previously installed/activated for that IP-CAN bearer.

If the PCRF decides to remove all PCC rules bound to an IP CAN bearer due to an internal trigger or trigger from the SPR, the PCRF shall instantly remove/deactivate all the PCC rules that have been previously installed/activated on that IP-CAN bearer.

If no more PCC rules are applied to an IP CAN bearer, the PCEF shall terminate the IP CAN bearer.

A.3.7 Request of IP-CAN Session Termination

The procedure described in clause 4.5.9 applies with the following changes:

If no more PCC rules are applied to an IP CAN session, the PCEF shall send a PDP context deactivation request with the teardown indicator set to indicate that the termination of the entire IP-CAN session is requested.

If the selected Bearer Control Mode (BCM) is UE-only, and the PCRF receives a trigger for the removal of all PCC rules bound to an IP CAN session from the AF, the following steps apply. In order to avoid race conditions, the PCRF should start a timer to wait for the UE-initiated bearer termination message. If a UE-initiated bearer termination of an IP CAN session is performed before timer expiry, the PCRF will receive an Indication of IP-CAN Session Termination according to Clause A.3.5 and shall then not perform the network-initiated termination of that IP CAN session. Otherwise, if the timer expires, the PCRF shall remove/deactivate all the PCC rules that have been previously installed or activated for that IP-CAN session.

A.3.8 Bearer Control Mode Selection

The GGSN shall only include the Network-Request-Support AVP if it supports this procedure and both the UE and the SGSN have previously indicated to the GGSN (refer to 3GPP TS 23.060 [17] and 29.060 [18]) that they also support it. The Network-Request-Support AVP shall be included if the GGSN received it from the SGSN.

The PCRF derives the Selected Bearer-Control-Mode AVP based on the received Network-Request-Support AVP, access network information, subscriber information and operator policy. The Selected Bearer-Control-Mode AVP shall be provided to the GGSN using the PCC Rules provision procedure at IP-CAN session establishment. The GGSN should forward it to the UE. The selected value is applicable to all PDP Contexts within the activated PDP Address/APN pair.

The BCM selection procedure can also be triggered as a consequence of a change of SGSN.

The values defined in 5.3.23 for the Bearer-Control-Mode AVP apply with the following meaning:

UE_ONLY (0)

This value is used to indicate that the UE shall request any additional PDP Context establishment.

RESERVED (1)

This value is not used in this Release.

UE_NW (2)

This value is used to indicate that both the UE and PCEF may request any additional PDP Context establishment and add own traffic mapping information to a PDP Context.

A.3.9 Bearer Binding Mechanism

A mapping from the EPS bearer parameter ARP to the pre-Rel-8 bearer parameter ARP is not required for a P-GW when connected to an SGSN via Gn/Gp as any change of the bearer ARP parameter may get overwritten by the SGSN due to subscription enforcement. However, when the PDN GW is connected to an SGSN via Gn/Gp (and thus a handover from UTRAN/GERAN to E-UTRAN is possible), the bearer binding in the PCEF shall not combine PCC rules with different ARP values onto the same PDP context. For the UE-only mode (which is based on a UE provided binding) PCC rules with different ARP values shall not be authorized for the same PDP context.

A.3.10 Provisioning and Policy Enforcement of Authorized QoS

A.3.10.1 Overview

The PCRF may provide the authorized QoS that applies to a bearer to the PCEF. When the authorized QoS applies to an IP CAN bearer, it shall be provisioned outside a Charging-Rule-Definition AVP and it shall also include the Bearer-Identifier AVP to indicate what bearer it applies to.

If the PCRF performs the bearer binding, the authorized QoS per IP CAN bearer presents the QoS for this IP CAN bearer. Authorized QoS per QCI is not applicable. If the PCEF performs the bearer binding, the authorized QoS per IP CAN bearer is not applicable.

The Provisioning of authorized QoS per IP CAN bearer may be performed separate or in combination with the PCC rule provisioning procedure in Clause 4.5.2.

In case the PCRF provides PCC rules dynamically, authorised QoS information for the IP-CAN bearer (combined QoS) may be provided. For a predefined PCC rule within the PCEF the authorized QoS information shall take affect when the PCC rule is activated.

The PCEF shall make sure that the total QoS information of the PCC rules for one IP-CAN bearer does not exceed the authorized QoS information, i.e. the information received from the PCRF.

A.3.10.2 Provisioning of authorized QoS per IP CAN bearer

The authorized QoS per IP-CAN bearer is used if the bearer binding is performed by the PCRF (as defined in [8]).

The PCEF will request the authorization of an IP CAN bearer establishment or modification by the PCRF using the "Request for PCC rules" procedure if the related conditions outlined in Clause 4.5.1 apply. While executing this procedure, the PCEF shall apply the following QoS related procedures:

- When the UE request the establishment of a new IP-CAN bearer, the PCEF shall derive the requested QoS information and shall request a new PCC decisions using a CCR command including the requested QoS information within the QoS-Information AVP, in the CCR command to be sent to the PCRF.

  The PCEF shall then wait for the corresponding CCA before replying to the IP-CAN bearer establishment request.

- If at any point of time the PCEF receives a request for a modification of an already existing IP-CAN bearer that matches event triggers supplied by the PCRF for the IP CAN session, the PCEF shall also request a new PCC decisions using a CCR command including the corresponding event triggers in the Event-Trigger AVP. If a QoS change for the existing IP-CAN bearer is requested the PCEF shall include the requested QoS information within the QoS-Information AVP in the CCR.

  The PCEF shall wait for the corresponding CCA before replying to the IP-CAN bearer modification request.

When receiving a CCR with a QoS-Information AVP, the PCRF shall decide upon the requested QoS information within the CCR command.

- The PCRF may compare the authorized QoS derived according to Clause 6.3 of 3GPP TS 29.213 with the requested QoS. If the requested QoS is less than the authorised QoS, the PCRF may either request to upgrade the IP CAN QoS by supplying that authorised QoS in the QoS-Information AVP to the PCEF (e.g. if the PCRF has exact knowledge of the required QoS for the corresponding service), or the PCRF may only authorise the requested QoS by supplying the requested QoS in the QoS-Information AVP to the PCEF (e.g. if the PCRF only derives upper limits for the authorized QoS for the corresponding service). If the requested QoS is higher than the authorised QoS, the PCRF shall downgrade the IP CAN QoS by supplying the authorised QoS in the QoS-Information AVP to the PCEF.

If for any reason the PCRF cannot authorize the requested QoS (e.g. authorized QoS would exceed the subscribed QoS), the PCRF shall indicate to the PCEF that the request is rejected by answering with a CCA command including the Experimental-Result-Code AVP set to the value DIAMETER_ERROR_BEARER_NOT_AUTHORIZED (5143) together with the bearer-identifier AVP. Otherwise, the PCRF shall provide a response for the CCR to the PCEF by issueing a CCA command without this experimental result code. The PCRF may use this CCA at the same time for the solicited PCC rule provisioning procedure in Clause 4.5.2. The CCA command shall include a QoS-Information AVP at command level including the Bearer-Identifier AVP used in the corresponding CCR and the authorized QCI and bitrates. If PCRF decides to move rules between bearers, the CCA command shall also include the QoS-Information AVP(s) for the impacted bearers.

The PCRF may also decide to modify the authorized QoS per IP CAN bearer if it reveives a CCR with other event triggers, for instance if the PCRF moves PCC rules from one IP-CAN bearer to another (e.g. in GPRS due to a TFT change). The PCRF shall then provision the updated authorized QoS per IP CAN bearer in the CCA within a QoS-Information AVP at command level including the corresponding Bearer-Identifier AVP.

The PCRF may decide to modify the authorized QoS per IP CAN bearer at any time. However, if the QoS-Upgrade AVP has been received by the PCRF indicating that QoS upgrade is not supported, the PCRF shall not upgrade the authorized QoS. To modify the authorized QoS per IP CAN bearer, The PCRF shall send an unsolicited authorization to the PCEF. The unsolicited authorization shall be performed by sending a RAR command to the PCEF and including the

QoS-Information AVP(s) with the new authorized values per IP CAN bearer. The PCRF may use this RAR at the same time for the unsolicited PCC rule provisioning procedure in Clause 4.5.2. If the trigger to modify the authorized QoS comes from the AF, before starting an unsolicited provisioning, the PCRF may start a timer to wait for a UE requested corresponding PDP context modification. At the expiry of the timer, if no PCC rule request has previously been received by the PCRF, the PCRF should go on with the unsolicited authorization as explained above.

In addition to a provisioning of the "Authorized QoS" per IP CAN Bearer, the PCRF may also provide an authorized QoS per PCC rule.

A.3.10.3 Policy enforcement for authorized QoS per IP CAN bearer

The PCEF is responsible for enforcing the policy based authorization, i.e. to ensure that the requested QoS is in-line with the "Authorized QoS" per IP CAN Bearer.

If the PCEF receives a solicited authorization decision from the PCRF (i.e. a decision within a CCA) and the requested QoS received within the IP-CAN bearer establishment or modification request that triggered the corresponding request for the authorization decision does not match the authorised QoS, the PCEF shall adjust the requested QoS information to the authorised QoS information within the IP-CAN bearer establishment or modification response.

The PCEF may store the authorized QoS of an active IP-CAN bearer in order to be able to make local decisions, when the UE requests for an IP-CAN bearer modification.

When the PCEF receives an unsolicited authorisation decision from the PCRF (i.e. a decision within a RAR) with updated QoS information for an IP-CAN bearer, the PCEF shall update the stored authorised QoS.If the existing QoS of the IP-CAN bearer does not match the updated authorised QoS the PCEF shall perform a network initiated IP-CAN bearer modification to adjust the QoS to the authorised level.

If the PCEF provide authorized QoS for both, the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules shall take place first.

A.3.10.4 Policy provisioning for authorized QoS per service data flow

If the PCRF performs the bearer binding for a service data flow, the PCRF may optionally provision an authorized QoS for that service data flow.

A.3.10.5 Policy enforcement for authorized QoS per service data flow

If the PCRF provides authorized QoS for both, the IP-CAN bearer and PCC rule(s), the enforcement of authorized QoS of the individual PCC rules shall take place first.

A.3.10.6 Coordination of authorized QoS scopes in mixed mode

For mixed mode the PCEF will request the authorization of an IP CAN bearer establishment or modification by the PCRF using the "Request for PCC rules" procedure if the related conditions outlined in Clause 4.5.1 apply. The PCEF shall then substract the guaranteed bitrate for the PCC rule it has bound to that IP CAN bearer from the requested QoS of that IP CAN bearer and request the authorization of the remaining QoS from the PCRF within the within the QoS-Information AVP.

The PCRF shall authorize the bandwidth for an IP CAN bearer which is required for the PCC rules it has bound to this IP CAN bearer. The PCEF shall add to the PCRF-provisioned authorized bandwidth of an IP CAN bearer the required bandwidth of all PCC rules it has bound to that IP CAN bearer unless the derived MBR value exceeds a possibly provisioned authorized QoS per QCI for the bearerer´s QCI (see Clause 4.5.5.6).

A.3.10.7 Provisioning of authorized QoS per QCI

If the PCRF performs the bearer binding the PCRF shall not provision an authorized QoS per QCI.

A.4 QoS Mapping

A.4.1 QCI to QoS parameter mapping

The mapping of QCI to UMTS QoS parameters for GPRS is shown in the following table (coming from TS 23.203 [7] Annex A table A.3):

Table A.4.1.1: Mapping for QoS Class Identifier to/from QoS parameters

QoS-Class-Identifier AVP Value	UMTS QoS parameters			
	Traffic Class	**THP**	**Signalling Indication**	**Source Statistics Descriptor**
1	Conversational	n/a	n/a	speech (NOTE)
2	Conversational	n/a	n/a	unknown
3	Streaming	n/a	n/a	speech (NOTE)
4	Streaming	n/a	n/a	unknown
5	Interactive	1	Yes	n/a
6	Interactive	1	No	n/a
7	Interactive	2	No	n/a
8	Interactive	3	No	n/a
9	Background	n/a	n/a	n/a
NOTE: The QCI values that map to "speech" should be selected for service data flows consisting of speech (and the associated RTCP) only.				

Annex B (normative): Access specific aspects, 3GPP (GERAN/UTRAN/E-UTRAN) EPS

B.1 Scope

This annex defines access specific aspects procedures for use of Gx/Gxx between PCRF and a 3GPP EPC IP-CAN.

B.2 Functional Elements

B.2.1 PCRF

For GTP-based 3GPP and PMIP-based 3GPP EPS accesses, the PCRF may, based on SPR information and internal policies, authorize the AMBR per APN for both Gx and Gxx interfaces.

B.2.2 PCEF

For GTP-based 3GPP and PMIP-based 3GPP EPS accesses, the PCEF shall be able to enforce the AMBR per APN.

B.2.3 BBERF

For PMIP-based 3GPP EPS access, the BBERF shall be able to support the AMBR per APN.

B.3 PCC procedures

B.3.1 Request for PCC and/or QoS rules

For GTP-based 3GPP accesses, the PCEF may send, besides the information described in clause 4.5.1, the subscribed APN- Aggregate-Max-Bitrate-DL AVP and APN-Aggregate-Max-Bitrate-/UL AVP within the QoS-Information AVP at command level as part of the IP-CAN Session Establishment procedure and IP-CAN Session Modification procedure.

For PMIP-based 3GPP accesses, the BBERF may send, besides the information described in clause 4a.5.1, the subscribed APN-Aggregate-Max-Bitrate-DL AVP and APN-Aggregate-Max-Bitrate-UL AVP within the QoS-Information AVP at command level as part of the Gateway Control Session Establishment procedure and Gateway Control Session Modification procedure.

B.3.2 Provisioning of PCC and/or QoS rules

For 3GPP accesses, the PCRF may provision the authorized QoS per APN as part of the Provisioning of PCC and/or QoS rules procedures, according to clause B.3.3.1.

B.3.3 Provisioning and Policy Enforcement of Authorized QoS

B.3.3.1 Provisioning of authorized QoS per APN

For 3GPP accesses, the PCRF may provision the authorized QoS per APN.

The authorized QoS per APN shall be provisioned at RAR or CCA command level using the QoS-Information AVP withincluding the APN-Aggregate-Max-Bitrate-UL AVP and/or the APN-Aggregate-Max-Bitrate- DL AVP. When

APN-Aggregate-Max-Bitrate-UL AVP and/or the APN-Aggregate-Max-Bitrate- DL AVP are provided, the Max-Requested-Bandwidth values, and the Guaranteed Bitrate values and the bearer identifier shall not be filled upincluded.

The authorized QoS per APN may be provisioned via the Gx interface as part of the IP-CAN session establishment procedure and may be modified at any time as long as there is an IP-CAN session active for that APN. The authorized QoS per APN may be modified as part of the IP-CAN session establishment or modification of any of the IP-CAN sessions active for a UE within that APN. The last provided value will replace the old value associated with a certain UE and APN regardless of which IP-CAN session that it is being modified in case multiple IP-CAN sessions exist for the same APN. For PMIP-based 3GPP accesses, the authoroized QoS per APN will also be provisioned via the Gxx interface to the BBERF.

B.3.3.2 Policy enforcement for authorized QoS per APN

For 3GPP accesses, the PCEF may receive an authorized QoS per APN. It sets an upper limit for the bandwidth usage for all the non-GBR bearers for that APN. The PCEF shall limit to that value the aggregated traffic of all SDFs of the same APN that are associated with Non-GBR QCIs).

Annex C (informative): Change history

Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
11/11/2005					Includes the following TDOCs agreed at CT3#38: C3-050692, C3-050834, C3-050835, C3-050843, C3-050846	0.0.0	0.1.0
17/02/2006					Includes the following TDOCs agreed at CT3#39: C3-060130, C3-060131, C3-060132, C3-060140	0.1.0	0.2.0
12/05/2006					Includes the following TDOCs agreed at CT3#40: C3-060199, C3-060200, C3-060255, C3-060259, C3-060260	0.2.0	0.3.0
13/09/2006					Includes the following TDOCs agreed at CT3#41: C3-060378, C3-060379, C3-060382, C3-060434, C3-060438, C3-060439, C3-060441, C3-060443, C3-060445, C3-060536, C3-060551	0.3.0	0.4.0
09/11/2006					Includes the following TDOCs agreed at CT3#42: C3-060786, C3-060854, C3-060750, C3-060595, C3-060848, C3-060753, C3-060630, C3-060755, C3-060849, C3-060829, C3-060866, C3-060756, C3-060700, C3-060851	0.4.0	0.5.0
01/12/2006	TSG#33	CP-060636			Editorial update by MCC for presentation to TSG CT for information	0.3.0	1.0.0
22/02/2007					Includes the following TDOCs agreed at CT3#43: C3-070050, C3-070084, C3-070137, C3-070166, C3-070175, C3-070212, C3-070239, C3-070244, C3-070245, C3-070246, C3-070268	1.0.0	1.1.0
28/02/2007	TSG#35	CP-060097			Editorial update by MCC for presentation to TSG CT for approval	1.1.0	2.0.0
03-2007					MCC update to version 7.0.0 after approval at TSG CT#35	2.0.0	7.0.0
06-2007	TSG#36	CP-070419	001	1	IP-CAN session specific charging	7.0.0	7.1.0
06-2007	TSG#36	CP-070420	004	11	Handling of Authorized QoS	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	005	2	Subscription to notification of Loss of AF signalling	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	006	1	Routeing of Diameter commands - Gx	7.0.0	7.1.0
06-2007	TSG#36	CP-070420	007	5	QoS change event	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	008		PCC rule without Flow-Description AVP	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	009	1	Addition and removal of event triggers	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	010	2	Metering-Method AVP	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	011	2	Reporting-Level AVP	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	012	1	PCC-Rule-Status AVP	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	013		Charging-Information AVP	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	014	1	PCC-Rule-Event AVP	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	015		Corrections to Reused AVPs	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	016	4	Precedence AVP	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	017	6	Mixed Mode	7.0.0	7.1.0
06-2007	TSG#36	CP-070419	018	2	Correction to where binding should be	7.0.0	7.1.0
06-2007	TSG#36	CP-070420	024	1	Alignment of the QoS information	7.0.0	7.1.0
09-2007	TSG#37	CP-070555	025		Usage of Event-Trigger AVP in RAA	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	027		Correct inconsistent name of re-used AVPs	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	031	2	Combine different sets of authorized QoS information	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	033	1	Precedence of the PCC rule	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	034	3	Experimental-Result-Code for the IP-CAN session rejection	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	036	1	Several bearer QoS-Authorization AVP(s) in the same command	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	037	2	Bearer Identifier handling in Event Trigger reporting	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	039	2	Removal of Editor"s Notes	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	041	2	Location based PCC decisions and Event Triggers	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	042		IP-CAN Type AVP missing in commands	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	043	1	BCM change due to handover	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	048		Support of Authorisation Token in Gx	7.1.0	7.2.0
09-2007	TSG#37	CP-070556	049	3	Extension of IP-CAN-Type AVP to specify non-3GPP IP-CANs	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	051	1	Authorized QoS per QCI	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	052		Applicability to charging or policy control	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	053	2	IP-CAN bearer operation failure	7.1.0	7.2.0
09-2007	TSG#37	CP-070555	054		Gx Application Id	7.1.0	7.2.0
12-2007	TSG#38	CP-070726	056		Add Bearer-Identifier AVP in RAA message	7.2.0	7.3.0
			057		Alignment for the Indication of IP-CAN Bearer Termination Implications		
			058	5	Correction of default charging method over Gx interface		
			061	2	Clarify the ambiguous name of Max-Requested-Bandwidth-UL/DL AVPs		
			062	2	Authorized QoS per QCI provisioned in CCA		

			064	3	Modify the description of Charging-Rule-Report AVP		
			067	2	Adding 3GPP-User-Location-Info AVP in CCR message		
			068	1	Removing unnecessary and ambiguous text from the Charging-Rule-Install section		
			069		AVP applicability to charging or policy control		
03-2008	TSG#39	CP-080040	071		Adding clarification around the encoding of the IMEISV	7.3.0	7.4.0
03-2008	TSG#39	CP-080040	072	1	Reporting the current event related value by the event trigger	7.3.0	7.4.0
03-2008	TSG#39	CP-080040	073	1	PDP Session	7.3.0	7.4.0
03-2008	TSG#39	CP-080040	074		Metering method for online charging	7.3.0	7.4.0
03-2008	TSG#39	CP-080040	077	4	Support of access capabilities for QoS control in PCC	7.3.0	7.4.0
05-2008	TSG#40	CP-080292	100	2	Binding of PCC rules having no AF session	7.4.0	7.5.0
05-2008	TSG#40	CP-080292	101	2	Rejection of traffic mapping information	7.4.0	7.5.0
05-2008	TSG#40	CP-080292	102	1	Downgrading of QoS request	7.4.0	7.5.0
05-2008	TSG#40	CP-080299	78	1	Supporting tunneled and untunneled PCC rules	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	81		IP CAN session definition update	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	82	3	Event Report handling in Gx	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	86		Introduction of Gxx reference points	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	89	3	Gxx reference points overview	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	90	2	Gxx reference model	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	91	2	Quality of Service Control rule definition and operations	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	92	2	PCRF functional element for Gxx	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	93	1	BBERF functional element for Gxx	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	97	2	RAT type AVP	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	98	1	IP-CAN session termination procedures at Gxx	7.5.0	8.0.0
05-2008	TSG#40	CP-080299	99	1	IP-CAN session modification procedures at Gxx	7.5.0	8.0.0
09-2008	TSG#41	CP-080651	079	9	PCC Error Handling Procedures	8.0.0	8.1.0
09-2008	TSG#41	CP-080650	103	3	Update Gxx interface for Gateway relocation scenarios	8.0.0	8.1.0
09-2008	TSG#41	CP-080553	106	1	Removal of BCM=Nw-Init	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	107	1	ARP Handling in Gx	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	110	3	Completion of QoS rules request procedure in Gxx	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	114		Error code misalignments	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	117	3	Add CoA and tunnel related AVPs	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	118	1	Separation of GPRS specific procedures	8.0.0	8.1.0
09-2008	TSG#41	CP-080649	119	4	Use 3GPP-SGSN-MCC-MNC AVP for all accesses	8.0.0	8.1.0
09-2008	TSG#41	CP-080648	120	4	Gxx Application Id	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	124	1	Removing the unnecessary subclause	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	125	1	PCRF initiated gateway control session termination	8.0.0	8.1.0
09-2008	TSG#41	CP-080553	135	1	Missing AVP codes	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	136		Updates on Gxx reference point	8.0.0	8.1.0
09-2008	TSG#41	CP-080652	137	3	Gxx reused/specific AVPs	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	138	2	Gxx commands	8.0.0	8.1.0
09-2008	TSG#41	CP-080634	139	1	Add tunnel related AVPs	8.0.0	8.1.0
09-2008	TSG#41	CP-080553	145	2	Setting of Precedence in PCRF-initiated IP-CAN session modifcation	8.0.0	8.1.0
09-2008	TSG#41	CP-080553	149	1	Correction of RAA command	8.0.0	8.1.0
09-2008	TSG#41	CP-080553	151	4	Out of credit indication	8.0.0	8.1.0
12-2008	TSG#42	CP-080920	154	4	Gx and Gxx linking session	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	155	2	APN-AMBR in Gx and Gxx	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	157	1	New IP-CAN Type 3GPP-EPS and new RAT Type for E-UTRAN.	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	158	4	QoS-Rule AVP correction	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	159	2	Including QoS-Rules related AVPs in the procedures	8.1.0	8.2.0
12-2008	TSG#42	CP-080960	161	8	Time zone for Time Of Day	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	165	5	IP-CAN session termination initiated by PCRF	8.1.0	8.2.0
12-2008	TSG#42	CP-080768	166	1	Use 3GPP-SGSN-MCC-MNC AVP for all accesses	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	169	1	Tunnel information Handling over Gxx	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	170		RAA command over Gxx	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	173	1	Support for 3GPP2 BSID in Gx and Gxx	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	175	4	Event Triggers handling in Gxx	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	185	4	Change the format of ARP AVP	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	187	2	PCRF-initiated Gxx session termination (29.212)	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	190	2	Default QoS handling	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	192	2	BCM Selection in Gx and Gxx reference points	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	193		Clean-up of QoS handling procedures	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	194	2	Gxx tunnelling information description and use	8.1.0	8.2.0
12-2008	TSG#42	CP-080751	197	1	Additional failure codes in Rule-Failure-Code AVP	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	198	1	New AVP to convey SGW/AGW IP addresses over Gx/Gxx protocols	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	199	1	Additional Event Trigger	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	205		Clean-up of IP-CAN bearer and session termination procedures	8.1.0	8.2.0
12-2008	TSG#42	CP-080920	206	2	ARP Setting for Default Bearers	8.1.0	8.2.0

History

Document history		
V8.0.0	October 2008	Publication
V8.1.0	October 2008	Publication
V8.2.0	February 2009	Publication