3GPP TR 29.804 V8.0.1 (2008-12)

Technical Report

3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; CT WG3 aspect of 3GPP System Architecture Evolution: (Stage 3); Release 8

Keywords
SAE, EPS, LTE, EPC, PCC, QoS, interworking, MBMS

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

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.

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

The present document discusses and describes procedures and protocols from CT3 aspects of System Architecture Evolution (SAE) towards a higher-data-rate, lower-latency, packet-optimized system that supports multiple access technologies.

These CT3 aspects include the PCC enhancements (including impacts coming from the inter-access system handover, roaming and LBO), the QoS aspects for both 3GPP and non-3GPP networks, inter-working with external networks, MBMS and any other functions in the Evolved Packet Core (EPC) network that CT3 has impact on.

The present document is used as a placeholder for CT3 SAE materials to be moved to appropriate 3GPP technical specifications when it is sufficiently stable. As such, neither all the discussions within this document are finished nor the procedures need to be completed. This TR may also contain some empty clauses. This TR will no longer be updated on a systematic manner and therefore contained information may become outdated.

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

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

[2] 3GPP TS 23.401: "GPRS enhancements for E-UTRAN access".

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

[4] 3GPP TS 23.107: "Quality of Service (QoS) concept and architecture".

[5] 3GPP TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface".

[6] 3GPP TS 23.203: "Policy and charging control architecture".

[7] IETF RFC 2475: "An Architecture for Differentiated Services".

[8] 3GPP TS 23.003: "Numbering, addressing and identification".

[9] IETF RFC 2486: "The Network Access Identifier".

[10] IETF RFC 3261: "SIP: Session Initiation Protocol".

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

[12] 3GPP TS 29.212: "Policy and charging control over Gx reference point".

[13] 3GPP2 X.S0011-D: "cdma2000 Wireless IP Network Standard".

[14] 3GPP TR 29.909: "Diameter-based Protocol Usage and Recommendations in 3GPP".

[15] IETF RFC 2327: "SDP: Session Description Protocol".

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

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Subclause numbering depends on applicability and should be renumbered accordingly.

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Access Gateway (A-GW): The gateway functionality located in a non-3GPP access network where the policy enforcement should take place.

per APN Aggregate Maximum Bit Rate (APN-AMBR): The maximum bit rate that limits the aggregate bit rate of all Non-GBR bearers and all PDN connections of the same APN. Definition derived from 3GPP TS 23.401 [2].

per UE Aggregate Maximum Bit Rate (UE-AMBR): The maximum bit rate that limits the aggregate bit rate of all Non-GBR bearers of a UE. Definition derived from 3GPP TS 23.401 [2].

Editors Note: Whether UE-AMBR is used in PCC is FFS.

Evolved packet core network: the successor to the 3GPP Release 7 packet-switched core network, developed by 3GPP within the framework of Release 8.

Evolved packet system: The evolved packet system (EPS) or evolved 3GPP packet-switched domain consists of the evolved packet core network and the evolved universal terrestrial radio access network. Definition derived from 3GPP TS 23.401 [2].

Default bearer: An EPS bearer that is established when the UE connects to a PDN, and that remains established throughout the lifetime of the PDN connection to provide the UE with always-on IP connectivity to that PDN. Definition derived from 3GPP TS 23.401 [2].

Dedicated bearer: An EPS bearer that is the additional EPS bearer that is established to a PDN for which a Default bearer has already established for the same UE. Definition derived from 3GPP TS 23.401 [2].

GBR bearer: An EPS bearer that uses dedicated network resources related to a Guaranteed Bit Rate (GBR) value, which are permanently allocated at EPS bearer establishment/modification. Definition derived from 3GPP TS 23.401 [2].

Non-GBR bearer: An EPS bearer that uses network resources that are not related to a Guaranteed Bit Rate (GBR) value. Definition derived from 3GPP TS 23.401 [2].

PDN address: an IP address assigned to the UE by the Packet Data Network Gateway (PDN GW).

3.2 Symbols

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

Symbol format

<symbol> <Explanation>

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

A-GW	Access Gateway
BBERF	Bearer Binding and Event Reporting Function
DSCP	Differentiated services code point
ePDG	evolved Packet Data Gateway
P-GW	PDN Gateway
S-GW	Serving Gateway

4. Overview of CT3 Aspect of System Architecture Evolution

5. PCC Enhancements

From the stage 2 architecture pictures in [2] and [3], the PCC architecture can be extracted and simplified as drawn in the pictures as shown in the below:

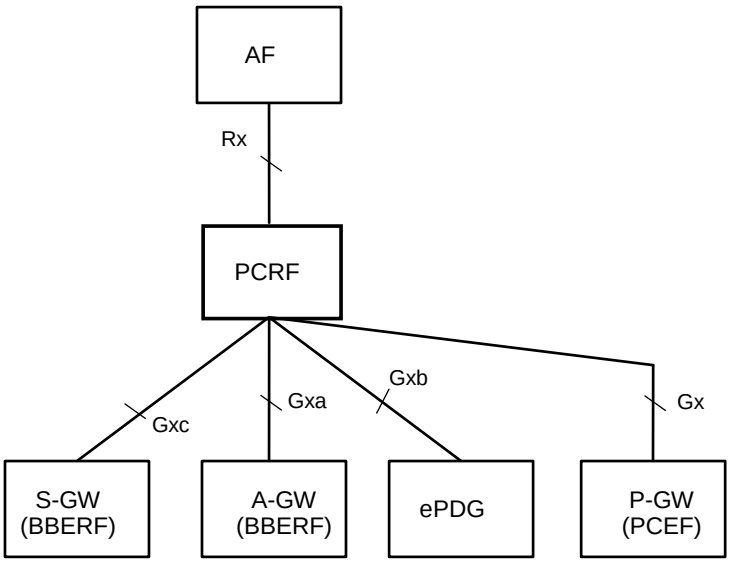

Figure 1: PCC architecture (non roaming)

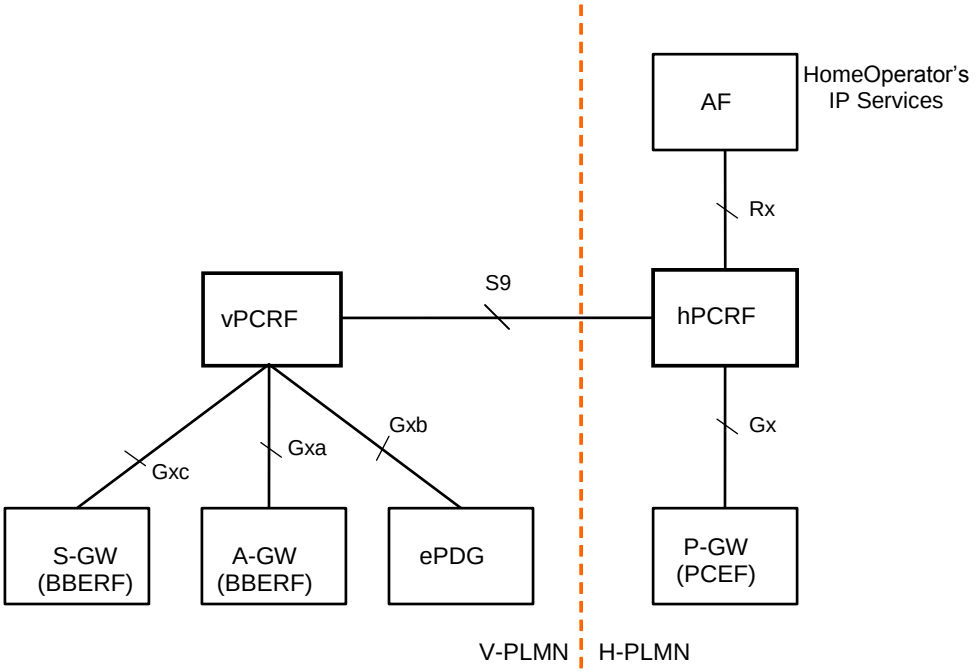

Figure 2: PCC roaming architecture for home-routed traffic

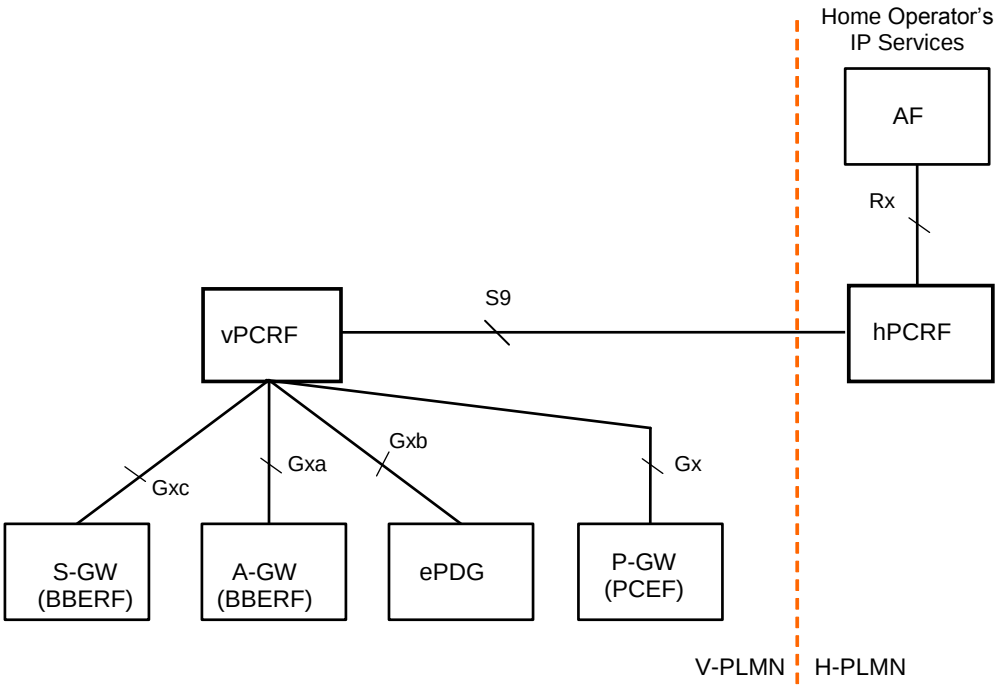

Figure 3: PCC roaming architecture for LBO with AF in the H-PLMN

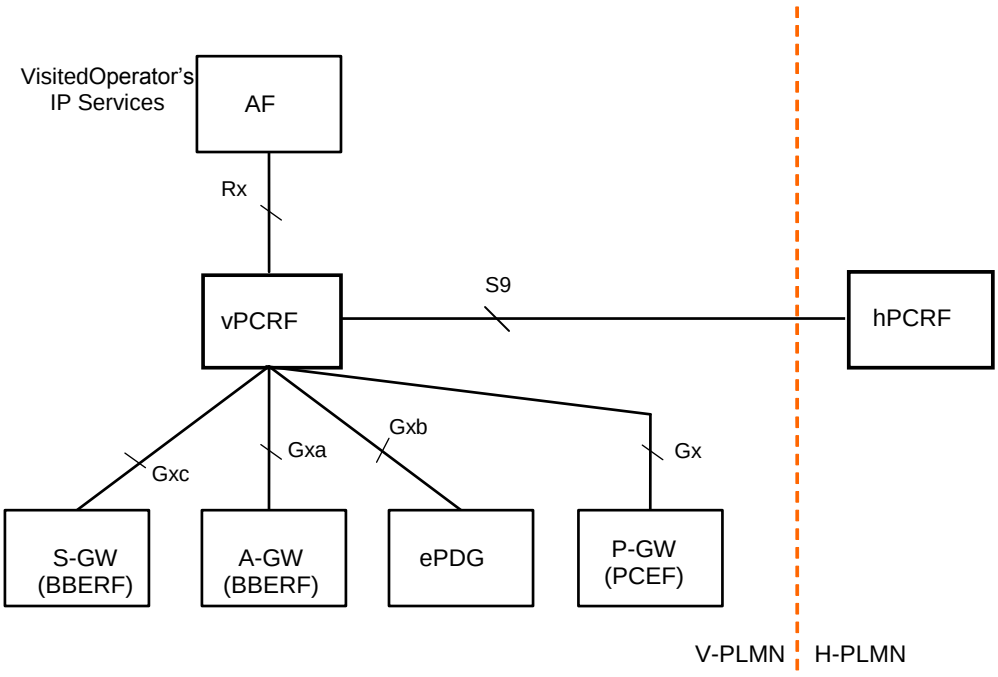

Figure 4: PCC roaming architecture for LBO with AF in the V-PLMN

The following interfaces are defined for PCC:

- Gx: based on Rel-7 Gx (Diameter). It is placed between the PCEF (located at the P-GW) and the PCRF (H-PCRF or V-PCRF). Gx supports all the functionality to install and remove PCC rules for policy and charging control.
- Gxa: based on Rel-7 Gx (Diameter). It is placed between the trusted non-3GPP A-GW (BBERF) and the PCRF (hPCRF or vPCRF). This interface is only used when the UE is using a trusted non-3GPP access network. PCC rules handling in Gxa is limited to policy and QoS information.
- Gxb: The details associated with the Gxb interface are not specified in this release.
- Gxc: based on Rel-7 Gx (Diameter). It is placed between the S-GW (BBERF) and the PCRF (hPCRF or vPCRF). This interface is only used in case that the UE is using a 3GPP access network and PMIP-based S5/S8b between the S-GW (BBERF)and the P-GW (PCEF). PCC rules handling in Gxc is limited to policy and QoS information.
- S9: based on Diameter. It is placed between the V-PCRF and the H-PCRF. It is used for exchanging session information and policy and charging information during roaming scenarios with either Local Break Out traffic or home-routed traffic.
- Rx: based on Rel-7 Rx (Diameter). It is placed between the AF and the PCRF (H-PCRF or V-PCRF) and is used to exchange session information. The AF and the PCRF communicating through the Rx interface are within the same network.

5.1 Functional Entities

5.1.1 AF

The AF (Application Function) is an element offering applications that require the Policy and Charging Control of traffic plane resources (e.g. EPC domain resources). One example of an application function is the P-CSCF.

The AF provides the session information to the PCRF based on signalling exchanged with the UE.

5.1.2 PCRF

5.1.2.1 General

PCRF encompasses policy and charging control decision functionalities to support the operator's IP services, e.g. IMS, PSS etc. The PCRF receives session information from the AF and informs AF of IP-CAN session events through the Rx interface. The PCRF provisions PCC rules to the PCEF in the PDN Gateway via the Gx interface (refer to 3GPP TS 23.401 [2]). The PCRF provisions QoS rules to the BBERF in the Serving Gateway via the Gxc interface in case of a PMIP based S5/S8 interface (refer to 3GPP TS 23.402 [3]) and to the BBERF of non-3GPP accesses via the Gxa and Gxb interfaces (refer to 3GPP TS 23.402 [3]). The PCRF determines whether a session towards the PCEF is to be linked with another session towards the BBERF by performing a matching of the IP address(es); the PCRF may also use the UE ID and PDN ID.

Editor's Note: According to stage2's procedures, IP address(es) could not always be available. For those cases, UE ID and PDN ID may be required in order to link sessions.

PCRF can support use cases with home routed traffic with IMS. Interworking between PCRFs is applicable via S9 interface e.g. to support routeing optimization such as local breakout scenario in the roaming architecture.

The PCRF can act as H-PCRF or V-PCRF depending of the location (H-PLMN or V-PLMN respectively).

There may be several PCRF entities in a network. A single PCRF entity within a PLMN shall be associated with all PCC sessions of a UE over different PCRF interfaces as described in subclauses 5.2 and 5.3 of the present TR.

5.1.2.2 H-PCRF

The H-PCRF (Home-Policy and Charging Rules Function) is a functional element that encompasses policy and charging control decision functionalities in the H-PLMN.

When home operator's AF is used and a UE is roaming in a visited network which applies policy control to the session(s) of the UE, the H-PCRF shall provision PCC rules to the V-PCRF through the S9 interface. Such roaming scenarios are e.g. a local breakout scenario (refer to 3GPP TS 23.401 [2] and 23.402 [3]) and a home routed scenario where the Serving Gateway employs a policy enforcement point and is controlled by the V-PCRF (refer to 3GPP TS 23.402 [3]).

5.1.2.3 V-PCRF

The V-PCRF (Visited-Policy and Charging Rules Function) is a functional element that encompasses policy and charging control decision functionalities in the V-PLMN..

When home operator's AF is used with a local breakout scenario (refer to 3GPP TS 23.401 [2] and 23.402 [3]) or with the Serving Gateway employing a policy enforcement point e.g. in a home routed scenario (refer to 3GPP TS 23.402 [3]), the V-PCRF obtains PCC rules from the H-PCRF through the S9 interface. The V-PCRF may reject the authorized QoS received from the H-PCRF based on operator policies (refer to 3GPP TS 23.401 [2] and 23.402 [3]).

Editor's note: Stage 2 does not clarify how the charging rules possibly sent by the H-PCRF to the V-PCRF should be handled by the V-PCRF. For example, the H-PCRF could possibly deliver charging specific subscription information like default charging method (online/offline). On the other hand, the VPLMN knowing the rating could mean that the V-PCRF generates the charging rules.

Editor's note: It is open whether the V-PCRF should be able to change the QoS, e.g. by downgrading, instead of simply rejecting the authorized QoS received from the H-PCRF.

5.1.3 PCEF

The PCEF (Policy and Charging Enforcement Function) is a functional element that encompasses policy and charging enforcement functionalities.

5.1.4 DRA

The DRA (Diameter Routing Agent) is a functional element that ensures that all Diameter sessions for Gx, S9, Gxa/c and Rx for a certain IP-CAN session reach the same PCRF when multiple and separately addressable PCRFs have been deployed in a Diameter realm. The DRA is not required in a network that deploys a single PCRF per Diameter realm.

5.1.5 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 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 untunnelled SDFs: The BBERF uses service data flow filters received from the PCRF for service data flow detection.

5.2 Procedures

5.2.1 General

Editor's Note: The UE may have been assigned more than one IP address. How to cover this fact in the Gx interface is FFS.

5.2.2 IP-CAN session establishment

5.2.2.1 General

This procedure is performed in the case of Attach, UE-requested additional PDN connectivity.

This procedure contains the following flows

- Interface Gxa/c:
  - Gateway Control Session Establishment. The S-GW/A-GW requests a new gateway control session to the PCRF. Then the PCRF authorizes the session and sends the corresponding QoS rules.
- Interface S9:
  - Gateway Control Session Establishment. The V-PCRF forwards an indication of a Gateway Control Session Establishment to the H-PCRF.
  - IP-CAN session establishment. For Local Breakout scenario, the V-PCRF forwards an indication of IP-CAN session establishment from the PCEF to the H-PCRF. The H-PCRF provisions the corresponding PCC rules. The V-PCRF forwards the PCC rules provisioned by the H-PCRF to the PCEF. If the BBERF is deployed, it extracts the QoS rules from the PCC rules provisioned by the H-PCRF and provisions them on the BBERF if applicable (i.e. current QoS rules on BBERF don't match QoS rules extracted from PCC rules received over S9).

Editor's note: It is FFS whether Gxx messages will be forwarded over the S9 reference point, i.e. QoS rules will be requested from the H-PCRF, in which case, extraction of QoS rules from PCC rules may not be needed.

- Interface Gx:

- Indication of IP-CAN session establishment. The PCEF indicates to the PCRF that the IP-CAN session has been established. As a response the PCRF can install the corresponding PCC rules.
- Policy and Charging Rule provision. The PCRF provisions the needed PCC rules to the PCEF.

5.2.2.2 Procedures over Gxa/Gxc

5.2.2.2.1 Gateway control session establishment

The BBERF shall send a CC-Request with CC-Request-Type AVP set to the value "INITIAL_REQUEST". The BBERF shall also supply user identification (eg. MN NAI) and other attributes to allow the PCRF (home or visited) 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, for 3GPP EUTRAN, 3GPP2 HRPD) if available, and the IP address(es). In addition, information about the user equipment (e.g. IMEISV), QoS negotiated, A-GW/S-GW address(es), country and network codes, APN if available, TFT and IMS signalling indication (if available) shall be provided.

Editor's Note 1: It is FFS whether there are procedures required to identify the requested resources, eg. addition of Resource-Id, Resource-Operation parameters

Editor's Note 2: It is FFS which of the aforementioned parameters will be needed by the PCRF for QoS and PCC rules decision

Editor's Note 3: It is FFS which of the aforementioned parameters will be common and which access specific (eg. specific 3GPP, 3GPP2, WiMAX parameters)

The PCRF shall provision QoS rules in the CC-Answer. 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 session establishment that initiated the CC Request

5.2.3 IP-CAN session modification

5.2.3.1 General

This procedure is performed in the case of Dedicated Bearer establishment, modification, and Deactivation or default bearer modification. It may also happen in case of UE-initiated resource request and release. It may also happen when Tracking Area Update (TAU), NW node Relocation (e.g. Intra-LTE TAU and Inter-eNodeB Handover with CN Node Relocation), and handover between 3GPP access and Non-3GPP access

This procedure contains the following flows

- Interface Gxa/c:
  - Gateway Control and QoS Rules Provision. The PCRF provisions the needed QoS rules to the BBERF, (see 5.4.1 in [3]).
  - Gateway Control Session Establishment. The BBERF requests a new gateway control session to the PCRF. This procedure is used when a TAU or a handover takes place.
  - Gateway Control Session Termination. The BBERF requests a termination of a gateway control session to the PCRF. This procedure is used when TAU or handover takes place.
  - Gateway Control and QoS Rules Request/Reply/Ack. The BBERF informs the PCRF of a condition (e.g. RAT change) that could require new policy and control rules provisioning. And then the PCRF installs/activates the needed QoS rules to the BBERF. (5.4.5.3, 5.5 and 5.7.2 in [3])
- Interface S9:
  - Policy and Charging Rule provision. The H-PCRF sends a request to provision the needed QoS rules in the BBERF to the V-PCRF. For Local Breakout scenario, the H-PCRF sends the needed PCC rules

to the V-PCRF; the V-PCRF extracts QoS rules and provisions them on the BBERF and provisions PCC rules on the PCEF.

- Gateway Control and QoS Rules Request/Reply/Ack. The V-PCRF forwards a request for PCC Rules to the H-PCRF.
- Gateway Control Session Establishment. The V-PCRF forwards an indication of a Gateway Control Session Establishment to the H-PCRF.
- Gateway Control Termination. The V-PCRF forwards an indication of termination of a GW Control Session to the H-PCRF.
- Request Policy and Charging Rules. For Local Breakout scenario, the V-PCRF forwards the request sent from the PCEF that could require new policy and charging control rules provisioning to the H-PCRF.
- Application/Service Info provision. For LBO scenario when AF is located in V-PLMN, the Rx information shall be forwarded by V-PCRF via S9 interface to H-PCRF and an acknowledgement is responded to the AF.

Editor's note: It is FFS whether Gxx messages will be forwarded over the S9 reference point, i.e. QoS rules will be requested from the H-PCRF, in which case, extraction of QoS rules from PCC rules may not be needed.

- Interface Gx:
  - Policy and Charging Rule provision. The PCRF provisions the needed PCC rules to the PCEF.
  - Request Policy and Charging Rules. The PCEF informs the PCRF of a condition that could require new policy and charging control rules provisioning.

5.2.3.2 Procedures over Gxa/Gxc

5.2.3.2.1 Gateway control and QoS Rules provision

The PCRF may decide to provision or update 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. No CCR/CCA messages are triggered by this RA-Request.

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 Gx experimental result code DIAMETER_PCC_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.

5.2.3.2.2 Gateway control session establishment

The procedures defined over clause 5.2.2.2.1 apply

5.2.3.2.3 Gateway control session termination

The procedures defined over clause 5.2.4.1.1 apply.

5.2.3.2.4 Gateway control and QoS Rules request

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 PCC rule(s) affected by the gateway control and QoS Rules request. The QoS Rules and their status shall be supplied to the PCRF within the Charging-Rule-Report AVP.

The PCRF shall provision QoS Rules in the CC-Answer. 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 that initiated the CC Request.

If the CC-Answer contained new and/or modified QoS rules, the BBERF shall send a CC-Request to acknowledge whether the resources requested have been successfully allocated.

Editor's Note: It is FFS how to communicate the result of allocating the resources.

Editor's Note: It is FFS in stage 2 if this message is sent for all QoS rules changes or if the conditions for sending it can/should be further refined.

The PCRF shall reply with a CC-Answer.

5.2.3.2.5 Gateway control session relocation

Gateway control session relocation occurs as a sequence. The new BBERF first establishes a Gateway Control Session as described in subclause 5.2.2.2.1. Then the old BBERF terminates its Gateway Control Session as described in subclause 5.2.4.1.1.

NOTE: Between the conclusion of the first step (establishing a new session) and the second step (terminating the old session), there will be more than one Gateway Control Session Active.

Editor's Note: It is FFS how PCRF-initiated gateway control session termination applies to the above case.

5.2.4 IP-CAN session termination

5.2.4.1 General

This procedure is performed the last active bearer within the IP-CAN session is deactivated or upon a UE detach from the network.

This procedure contains the following flows

- Interface Gxa/c:
    - Gateway Control Session Termination. The BBERF requests a termination of a Gateway Control session to the PCRF. This procedure is used when detaching in S2a and PMIP-based S5 case.
    - Gateway Control and QoS Rules Provision. The PCRF removes any active QoS rules referring to the Home Address in the BBERF. This procedure is used when disconnecting from a PDN in S2c case.

      NOTE: If no QoS rules remain in the Trusted Non-3GPP Access, the Trusted Non-3GPP Access terminates the gateway control session towards the PCRF.
    - PCRF-initiated Gateway Control Session Termination. This procedure is used in case the UE is detached and the CoA acquired by the UE is not used for any other IP-CAN Session.

Editor's Note: It is FFS that how PCRF determines that the Gateway Control Session shall be terminated.

- Interface S9:
    - Gateway Control Session Termination. The V-PCRF sends a request to terminate a GW control session to the H-PCRF. This procedure is used when disconnecting from a PDN and when detaching in S2a and PMIP-based S5 case.
    - Gateway Control and QoS Rules Provision. The H-PCRF removes any active QoS rules referring to the Home Address in the BBERF via the V-PCRF. This procedure is used when disconnecting from a PDN in S2c case, and the Gateway Control Session shall remain to server other IP-CAN Session.

      NOTE: If no QoS rules remain in the Trusted Non-3GPP Access, the Trusted Non-3GPP Access terminates the gateway control session towards the PCRF.

- PCRF-initiated Gateway Control Session Termination. This procedure is used in case the UE is detached and the CoA acquired by the UE is not used for any other IP-CAN Session.

Editor's Note: It is FFS that how PCRF determines that the Gateway Control Session shall be terminated.

- Indication of IP-CAN session termination. For Local Breakout scenario, the V-PCRF forwards an indication of IP-CAN session termination from the PCEF to the H-PCRF.

Editor's Note: The current procedures in stage 2 for LBO are FFS. The exact functional description has to be aligned with stage 2 decisions later.

- Interface Gx:
  - Indication of IP-CAN session termination from the PCEF to the PCRF.

5.2.4.2 Procedures over Gxa/Gxc

5.2.4.2.1 Gateway Control Session Termination

For detaching in S2a and PMIP-based S5 case, 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.

When S2c applies and the PCRF determines that the Gateway Control Session shall be terminated (e.g. No PDN connections), the PCRF shall initiate the Gateway Control Session Termination procedure.

Editor's Note: Which messages does PCRF use to initiate the Gateway Control Session Termination procedure is FFS.

5.2.4.2.2 Gateway control and QoS Rules provision

The procedures defined in subclause 5.2.3.2.1 apply.

5.2.5 PCRF discovery procedures

5.2.5.1 General

The PCRF discovery procedures are needed where more than one PCRF are present in an operator's network realm. When this deployment occurs an additional functional element, called DRA, is needed. PCRF discovery procedures include all the procedures that involve a DRA functional element

Routing of Diameter messages from a network element towards the right Diameter realm in a PLMN is based on standard Diameter realm-based routing, as specified in IETF RFC 3588 [11] using the UE-NAI domain part.

Having the same PCRF for all the involved interfaces will allow having all of the messages related to an IP-CAN session from different interfaces, e.g. Gx, S9, Gxa/c and Rx interfaces, routed to the same PCRF.

5.2.5.2 DRA Diameter functionality analysis and conclusion

This clause contains a comparison between Redirect Diameter Agent and proxy Diameter Agent. The main goal is to identify the pros and cons for the candidate solutions and select the most suitable one as the recommended DRA implementation.

NOTE: Other types of Diameter agents are not considered since they do not satisfy the DRA requirements in stage 2

5.2.5.2.1 Analysis

This clause includes the different issues that are evaluated for each of the candidate solutions. The issues include latency, load, scalability, reliability, security, deployment, how to maintain the session state and impacts on existing protocols nodes and standard Diameter agent.

A final analysis is done for the specific scenario where two operator networks are interconnected and using different DRA solutions (i.e. one operator uses a redirect solution while the other one uses the proxy one).

The following definitions apply:

Client: PCC functional nodes that act as a Diameter client: BBERF, PCEF, AF, V-PCRF

DRA Binding: The assignment of a PCRF node per UE or per IP-CAN Session

In this clause the examples are referred to the Gx interface for simplicity. These examples are equally applicable to the other interfaces: S9, Gxx and Rx.

The following solutions are compared:

[RA]: Redirect agent based on the standard Diameter redirect agent functionality. The deletion of the DRA binding is performed when the client is sending the session termination message to the DRA. After receiving the redirection message, the client will send it to the server. A possible optimization for this case would be that the same message is sent in parallel to the PCRF, having this the drawback of modifying the standard redirection mechanism in the client for such a particular case..

[PA1]: Proxy agent based on the standard Diameter proxy agent functionality. All the messages need to go through the DRA.

[PA2]: Proxy agent based on the standard Diameter proxy agent functionality. Only establishment and termination messages go through the DRA.

A proxy agent is not required to be on the route path of every subsequent command for a given Diameter session. The answer message for the initial Diameter command exchange contains the Origin-Host AVP and Origin-Realm AVP which can be used by the client to route subsequent commands directly to the destination host that processed the initial request. Alternatively the client could use the Origin-Realm AVP and Diameter realm-based routing to determine an alternate route to the destination host which bypasses the failed DRA cluster.

The following assumptions are taken into account:

1. The DRA has the all the functionality needed to handle the PCRF selection per either UE or PDN network. The client then would have the same behaviour in all the cases, i.e. each session establishment procedure will have to go to the DRA first to find out what PCRF is to be assigned.

5.2.5.2.1.1 Latency

The following definitions apply:

t: Processing time in the PCRF, e.g. time between receipt of a CCR and reply with CCA.

x: Time for a message to go from one Diameter node/agent to another node/agent. To simplify we consider this to be a constant.

z: Processing time unit in a Diameter agent. It is considered that when DRA binding is created/deleted the processing time is “2z”. When binding is not needed to be modified, the processing time is set to “z”

The following assumptions are taken into account:

2. the Diameter connections between the client/servers and the Diameter agents are pre-established and therefore are not being counted

3. For the comparison we may assume that t>>x, t>>y

5.2.5.2.1.1.1 Session Establishment

[RA]

- (+) Latency = 4x + 2z + t. The procedure is completed after four interactions. E.g. for the Gx interface, the CCR goes from the client to the DRA. DRA resolve the destination address and issue a CCA to the client. The client send the CCR directly to the PCRF and the PCRF answers back with the corresponding CCA.

[PA1]

- (+) Latency = 4x + 2z + t. The procedure is completed after four interactions. E.g. for the Gx interface, the CCR goes from the client to the DRA. DRA analyses it and send it to the final destination (PCRF). The PCRF answers back with a CCA that is sent to the DRA. The DRA analyses it and send it to the final destination (the client that issued the initial CCR)

[PA2]

- (+) Latency = 4x + 2z + t. E.g. for the Gx interface the answer (CCA) can go directly from the PCRF to the client without going through the DRA

5.2.5.2.1.1.2 Session Modification

[RA]

- (+) Latency = 2x + t. The procedure is completed after two interactions. The client already knows the PCRF address and uses it since there is no need to resolve it again in the DRA. The CCR goes directly from the client to the final destination, as the client already got the final address during the session establishment procedure. The answer also goes from the PCRF directly to the client.

[PA1]

- (-) Latency = 4x + z + t. The clients (BBERF, PCEF, AF, V-PCRF) obtain the answer of the operation in four interactions. The CCR goes from the client to the DRA. DRA analyses it and send it to the final destination (PCRF). The PCRF answers back with a CCA that is sent to the DRA. The DRA analyses it and send it to the client. Although latency in this case is higher than in the [RA] or [PA2] case (difference is 2x), it is important to look at the percent increase relative to the [RA] or [PA2] latency. The percentage increase is 2x*100/(2x+t). Because processing time in the PCRF is most likely higher than message travelling time, we can assume that t >> x, in which case, the percentage increase in latency in this case is minimal compared with the latency of the [RA] or [PA2] solutions.

[PA2]

- (+) Latency = 2x + t. The procedure is completed after two interactions. The client already knows the PCRF address and uses it without traversing the proxy agent.. The CCR goes directly from the client to the final destination, as the client already got the final address during the session establishment procedure. The answer also goes from the PCRF directly to the client.

5.2.5.2.1.1.3 Session Termination

[RA]

- (+) Latency = 4x + 2z + t. The procedure is completed after two interactions. E.g. for the Gx interface, The CCR goes directly from the client to the final destination, as the client already got the final address during the session establishment procedure. The PCRF answers back with the corresponding CCA. In parallel to this procedure, the client shall send the same CCR to the DRA in order for the DRA to remove the binding.

[PA1]

- (+) Latency = 4x + 2z + t. The procedure is completed after four interactions. E.g. for the Gx interface, the CCR goes from the client to the DRA. DRA analyses it and send it to the final destination (PCRF). The PCRF answers back with a CCA that is sent to the DRA. The DRA analyses it and send it to the final destination (the client that issued the initial CCR)

[PA2]

- (+) Latency = 4x +2z + t. E.g. for the Gx interface the answer (CCA) can go directly from the PCRF to the client without going through the DRA

5.2.5.2.1.2 Load

- In terms of number of messages (i.e. how many messages the DRA has to deal with)

  The analysis is simplified by making the following assumptions:

  ✓ Non-roaming case only

  ✓ No S-GW/A-GW relocation

  Additional assumptions:

  u: The number of session updates initiated by the UE/PCEF/BBERF as opposed to the PCRF-initiated updates.

  r: The number of Rx sessions established during an IP-CAN session

  r': The number of Rx sessions' modifications.

  p: The number of PCRF-initiated session updates.

  [RA]

  IP CAN Session Establishment:

  During an IP-CAN Session Establishment, a redirect agent has to process 4 messages (2 messages for GTP-based S5):

  1) Indication of IP CAN Session Establishment (from PCEF);
  2) Redirect indication to PCEF
  3) Gateway Control Session Establishment (from BBERF) (If Gxa/c apply)
  4) Redirect indication to BBERF

  IP CAN Session Modification:

  During IP-CAN session modification, only AF requests for Rx session establishment need to be processed by the DRA. As such, in this case, the DRA has to process 2r messages.

  IP CAN Session Termination:

  The DRA needs to process 4 messages (2 in the case of GTP-based S5) from the PCEF and the BBERF for session termination.

  [PA1]

  IP CAN Session Establishment:

  During an IP-CAN Session Establishment, a proxy agent has to process 8 messages (4 messages for GTP-based S5):

  1) Indication of IP CAN Session Establishment (from PCEF);
  2) Proxying the indication of IP-CAN Session Establishment to the PCRF
  3) Reply from the PCRF
  4) Proxying reply to the PCEF
  5) Gateway Control Session Establishment (from BBERF) (If Gxa/c apply)

6) Proxying the Gateway Control Session Establishment to the PCRF
7) Reply from the PCRF
8) Proxying reply to the BBERF

IP CAN Session Modification:

During an IP-CAN Session Modification, a proxy agent has to process (4u + 8r + 4r' + 4p) messages (4u = CCR(in&out) + CCA (UPDATE, in&out), 8r = AAR/AAA (session setup, in&out) + STR/STA (in&out), 4r' = AAR/AAA (in&out) for Rx session updates, 4p = Gx/a/c RAR/RAA (in&out) initiated by the PCRF).

IP CAN Session Termination:

The DRA needs to process 8 messages (4 in the case of GTP-based S5) from the PCEF and the BBERF for session termination.

[PA2]

IP CAN Session Establishment:

During an IP-CAN Session Establishment, a proxy agent has to process 8 messages (4 messages for GTP-based S5):

1) Indication of IP CAN Session Establishment (from PCEF);
2) Proxying the indication of IP-CAN Session Establishment to the PCRF
3) Reply from the PCRF
4) Proxying reply to the PCEF
5) Gateway Control Session Establishment (from BBERF) (If Gxa/c apply)
6) Proxying the Gateway Control Session Establishment to the PCRF
7) Reply from the PCRF
8) Proxying reply to the BBERF

IP CAN Session Modification:

During IP-CAN session modification, only AF requests for Rx session establishment need to be processed by the DRA. As such, in this case, the DRA has to process 2r messages.

IP CAN Session Termination:

The DRA needs to process 4 messages (2 in the case of GTP-based S5) from the PCEF and the BBERF for session termination.

Message loading conclusion:

IP-CAN session establishment and termination:

[RA]

(+)In this solution, 4 messages (2 in case of GTP-based S5) are processed in IP-CAN Session establishment and 4 messages (2 in case of GTP-based S5) are processed in IP-CAN Session Termination.

The RA solution performs less processing on IP-CAN session establishment than the other solutions as it does not forward the request or response but instead directly replies back to the client.

[PA1]/[PA2]

(-) In PA1 solution, 8 messages (4 in case of GTP-based S5) are processed in IP-CAN Session establishment and 8 messages (4 in case of GTP-based S5) are processed in IP-CAN Session Termination. In PA2 solution, 8 messages (4 in case of GTP-based S5) are processed in IP-CAN Session establishment and 4 messages (2 in case of GTP-based S5) are processed in IP-CAN Session Termination. The PA solutions perform additional processing as they need to proxy the request and the answer.

IP-CAN session modification message load summary:

[RA] / [PA2]

(+) In this solution, 2r messages are processed.

[PA1]

(-) In this solution, (4u + 8r + 4r' + 4p) are processed. The difference with the other solutions is (4u+6r+4r'+4p). The message load is definitely greater in this solution, however, one needs to note that the additional messages that are processed need minimal processing at the DRA, and are comparable to a relay agent processing requirements when forwarding/relaying messages.

- In terms of number of connections (i.e. how many connections are needed from the clients/servers)

Assumptions:

S: Number of servers in an operator's network (across all Diameter realms).

C: Number of clients in an operator's network (across all Diameter realms).

R: Number of realms with a DRA within an operator's network.

[RA]

1) Each client (GW/AF) needs a connection with the DRA;
2) Each client (GW/AF) needs a connection with the server (PCRF);

Each client may have to establish up to (R + S) connections.

Each PCRF may have to handle up to C connections.

The total number of connections required may be a full mesh, i.e. (R+S) * C, where every client may be connected with every server and DRA and vice-versa.

[PA1]

1) Each client (GW/AF) needs a connection with the DRA,
2) A client (GW/AF) does not need a direct connection with the server (PCRF);
3) The server needs a connection with DRA; (1 connection)

Clients only need to establish R connections to all of the DRAs. Servers need to only establish one connection to the DRA in their realm. The total number of connections is (C*R + S) for the entire operator's network (across all realms).

[PA2]

1) Each client (GW/AF) needs a connection with the DRA;

2) Each client (GW/AF) needs a connection with the server (PCRF);

3) Each server needs a connection with DRA; (1 connection)

This is similar to the connection requirements on the [RA] with an additional connection from each PCRF to the DRA. The total number of connections is (S+R)*C+S.

Connection load conclusion:

(-) [RA]: This solution requires (R+S) connections from the client side and C connections from the server side and a total of (R+S) * C connections for the entire operator's network. This solution imposes greater connection related load on the clients, servers and network as a whole. The total number of connections between clients and servers is not linear relatively to the number of clients and servers in an operator's network, but is proportional to S*C.

(+) [PA1]: This solution requires the least amount of connection load on the clients (R connections each) and servers (only one connection each). The total number of connections is (C*R + S) for the entire operator's network (across all realms). This solution requires S*(C-1) less connections than the [RA] solution. Additionally, the total number of connections grows linearly with the number of clients and servers, unlike the [RA]/[PA2] solutions.

(-) [PA2]: This solution requires S more conncetions than [RA] solution., which is similar to the connection requirements on the [RA] with additional connections from each PCRF to the DRA. As such, this solution is comparable to the [RA] solution from a connection load basis.

5.2.5.2.1.3 Scalability

From a scalability point of view redirect-DRAs [RA], proxy-DRA variant [PA1] and proxy-DRA variant [PA2] could be deployed as clusters that all share a common memory bank or database. Load balancing mechanisms could be implemented to distribute requests between active DRA-nodes in such a cluster. As a result all three options could be implemented to scale and to provide redundancy as transaction load increases.

The following section analyses the transport connection requirements per element for each solution. The connection per element refers only to the additional connections required for DRA functionality and not to the total number of connections required for all element functions.

Connections per client (AF, PCEF or BBERF):

- [RA]: Each client requires a connection to every DRA and every PCRF.
- [PA1]: Each client requires a connection to every DRA.
- [PA2]: Each client requires a connection to every DRA and every PCRF.

Connections per DRA:

- [RA]: Each DRA requires a connection to every client.
- [PA1]: Each DRA requires a connection to every client and to every PCRF associated with this DRA.
- [PA2]: Each DRA requires a connection to every client and to every PCRF associated with this DRA.

Connections per PCRF:

- [RA]: Each PCRF requires a connection to every client.
- [PA1]: Each PCRF requires a connection to the DRA associated with this PCRF.
- [PA2]: Each PCRF requires a connection to every client and to the DRA associated with this PCRF.

The following figures illustrate the impact of the different solutions on the number of transport connections per client as the network expands by adding PCRF and DRA. In this example, the PCEF is initially using Diameter realm-based

routing to locate the appropriate DRA for realms A, B, C and D. Although a PCEF is used in this example, the client type (AF, PCEF, BBERF) is not a factor in the transport connection requirements. A PCRF to DRA ratio of 4:1 has been assumed in order to reduce the clutter in the figures but it may be much higher.

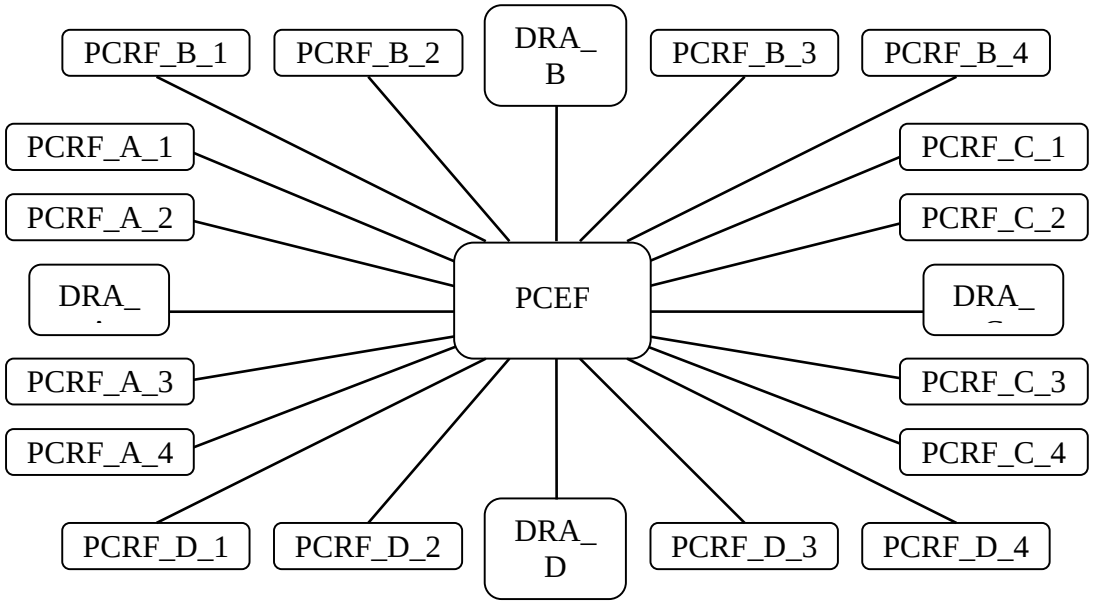

Figure 5.2.5.2.1.3.1: Solution [RA] Client Connections

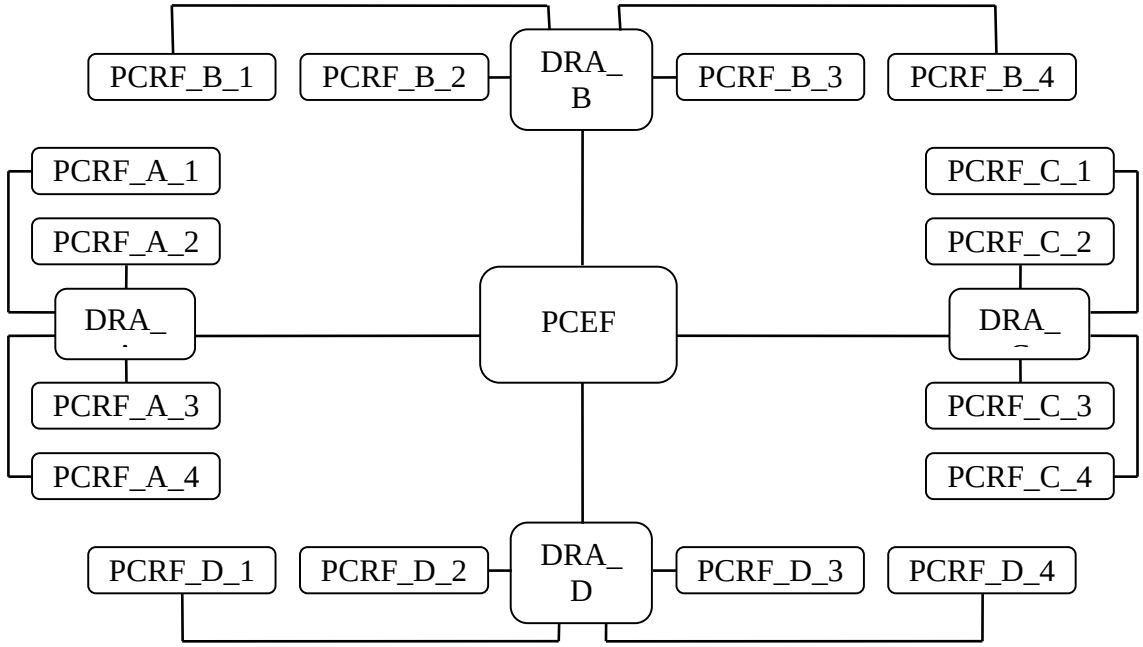

Figure 5.2.5.2.1.3.2: Solution [PA1] Client Connections

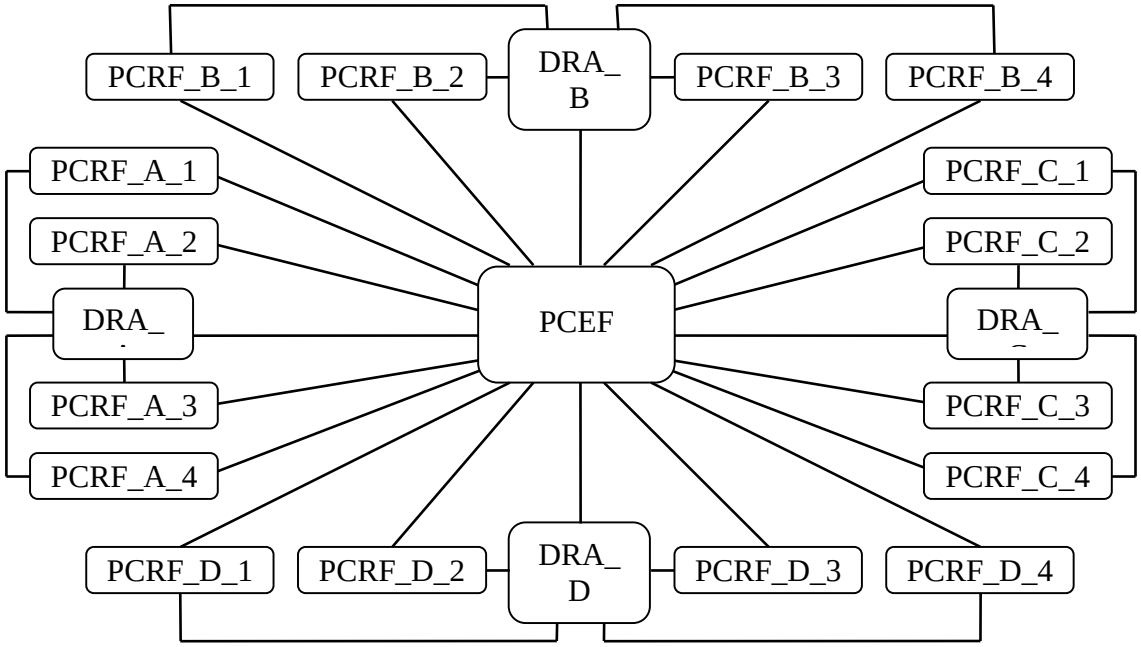

Figure 5.2.5.2.1.3.3: Solution [PA2] Client Connections

5.2.5.2.1.4 Reliability

In the case of a catastrophic failure of all DRA nodes in a cluster, the redirect-DRA may appear to be more reliable than proxy-DRA. If a redirect-DRA cluster experiences an outage, only the establishment of new sessions and termination of existing sessions is impacted. If a proxy-DRA cluster experiences an outage, it would appear that both existing and new sessions are impacted.

However, it is important to note that a proxy-DRA is not required to be on the route path of every subsequent command for a given Diameter session. The answer message for the initial Diameter command exchange contains the Origin-Host and Origin-Realm which can be used by the client to route subsequent commands directly to the destination host that processed the initial request. Hence, this proxy DRA variant [PA2] achieves the same level of reliability as the redirect DRA in this catastrophic failure scenario.

In the following analysis, it is assumed that the DRA Binding survives a DRA failure. If the DRA Binding is deleted on a DRA failure then the termination of existing sessions is not impacted in any of the candidate solutions.

Summarizing the impact of a catastrophic failure of all DRA nodes for each of the candidate solutions:

[RA]

- (+) No impact for ongoing sessions. The establishment of new sessions and termination of existing sessions is impacted.

[PA1]

- (-) The establishment of new sessions, modification of existing sessions and terminations of existing sessions is impacted.

[PA2]

- (+) No impact for ongoing sessions. The establishment of new sessions and termination of existing sessions is impacted.

In the case of failure of a single PCRF node, all ongoing sessions policed by the failed node are impacted regardless of the DRA solution being used. However, the redirect-DRA is unaware of the PCRF failure and would continue to redirect clients to the failed node impacting the establishment of new sessions. The proxy-DRA solutions ([PA1] and [PA2]) have a connection to the PCRF nodes allowing them to detect node failure and select an alternative PCRF for new sessions.

Summarizing the impact of a failure of a single PCRF node for each of the candidate solutions:

[RA]

- (-) All ongoing sessions are impacted and all new sessions redirected to the failed PCRF are impacted.

[PA1]

- (+) All ongoing sessions proxied to the failed PCRF are impacted. No impact on the establishment, modification or termination of new sessions.

[PA2]

- (+) All ongoing sessions proxied to the failed PCRF are impacted. No impact on the establishment, modification or termination of new sessions.

5.2.5.2.1.5 Security

NOTE: If Security gateways are used as defined in TS 33.210 [x] between operators (i.e. Za interface) and no security is needed for communication within a security domain (i.e Zb is not implemented and TLS is not used between peers), then, there would not be a disadvantage in using an ([RA] or [PA2]) v/s [PA1]. In the rest of the section, we assume that securing communication between Diameter peers is achieved as described in RFC 3588 [x] (e.g. TLS or IPSec between peers).

[RA]

(-) Security associations:

In roaming scenarios, if a home operator deploys the DRA as a redirect agent, each V-PCRF will connect directly with home PCRFs, thus, each home PCRF has to create a security association with all of the possible V-PCRFs and vice-versa. The more PCRFs in a Diameter realm, the more security-related configuration and management is needed as each PCRF has to be configured accordingly.

If security is needed within an operator's network, the disadvantage of such a solution is even greater as the number of direct connections between clients and servers is far greater than in the [PA1] approach, which burdens both clients and servers.

[PA1]

(+) Security associations:

Given that when the DRA is deployed as a proxy agent, it is the single entry point to the PCRF "cloud", security associations only need to be managed between the V-PCRF and the DRA in roaming scenarios. Also security related policies can be managed within one entity for incoming connections. Because there is only one DRA per realm, the number of security associations that need to be managed is far smaller than in the case of [RA] or [PA2].

The advantage of [PA1] compared to [RA]/[PA2] is even greater if security is needed within an operator's network as clients and servers have a connection only with the DRA, and given that there is only one DRA per realm, the number of security associations to manage is significantly less in the case of [PA1].

[PA2]

NOTE: From a security standpoint, [PA2] and [RA] are considered equivalent.

5.2.5.2.1.6 Deployment

- Non-roaming case

  [RA]

  - (-) Configuration at the PCRF: Every PCRF has a direct connection with every client (AF, PCEF, BBERF), and as such each time a new client is introduced, each PCRF has to be configured to allow connections from new peers (or not block connections from "unknown" peers).

- (+) Small deployments: In small deployments, the [RA] solution may be a simpler approach as it doesn't require an extra hop between clients and servers.

[PA1]

- (+) Configuration at the PCRF: Given that PCRFs have connections only with one DRA, there is no need to reconfigure the PCRF when new clients are introduced.
- (-) Small deployments: If an administrative realm only has very few PCRFs deployed, having a DRA in the path adds unnecessary overhead (additional hop).

[PA2]

Considered similar to [RA].

NOTE: If an internal pool of relays is used within one realm as defined in Annex A of TR 29.909, the differences between the different flavors becomes minimal.

- Roaming case

[RA]

- (-) Internal PCRF topology: Given that each PCRF in a home realm is connected directly with the roaming partner, the home operator would be opening up its internal topology to external networks. The visited PLMN's internal PCRF topology is not hidden in this case unless the visited PLMN deploys an outbound relay/proxy such that a V-PCRF does not connect directly with a home operator's DRA.
- (-) Network level policies: Given that there is no single entry point in this case to the PCRF "cloud", the operator cannot centrally manage policies related to the number or allowed peers with the PCRF "cloud", load.
- (+) Number of hops: The [RA] minimizes the number of hops at least for session modifications.

[PA1]

- (+) Internal PCRF topology: Given that the DRA in this case is the single entry point to the PCRF "cloud", a home operator can decide to hide its internal PCRF topology by only providing information about the DRA to an external network and not the selected PCRF. The visited PLMN's internal PCRF topology is not hidden in this case unless the visited PLMN deploys an outbound relay/proxy such that a V-PCRF does not connect directly with a home operator's DRA.
- (+) Network level policies: A home operator can deploy policies in one entity, the DRA, to manage incoming communication from roaming partners, such as allowed peers, number of connections and load from a particular operator or on an aggregate level, shielding the PCRFs from direct communication with external clients.
- (-) Number of hops: In the case of roaming, two hops are in the path for all messages: the V-DRA and H-DRA, such that a message from a client such as the BBERF for instance will need to traverse at least three hops before making it to the H-PCRF.

[PA2]

Similar to [RA].

NOTE: If an external pool of relays is used when interconnecting operators as defined in Annex A of TR 29.909, the differences between the different flavors becomes minimal.

5.2.5.2.1.7 Maintaining Session state

[RA]

- Aware of DRA binding states (eg. session establishment and termination). Not aware of all session states.

[PA1]

- Aware of DRA binding states. The Diameter Proxy agent keep track of theDRA binding state since it evaluates every packet that is sent between the client and the server

[PA2]

- Aware of DRA binding states (eg. session establishment and termination). Not aware of all session states. The PA2 option needs to receive the termination acknowledge messages (eg. CCA in a Gx CCR) in order to remove binding information.

5.2.5.2.1.8 Enhancement to the standard agents

This section describes the enhancements required on the standard redirect and proxy agent as defined in IETF RFC 3588

The DRA is required (see 23.203 Section 7.6) to ensure that all Diameter sessions for Gx, S9, Gxa/c and Rx for a certain IP-CAN session reach the same PCRF. This requirement implies that the DRA must maintain a PCRF Host to user name (e.g., NAI) binding.

> NOTE: An additional enhancement that is applicable to all options is that the DRA has to dynamically determine all subscriber identities (eg. PUIs) associated with a NAI (or IMSI if available) (e.g., by interrogating the subscriber data bases). This is to create NAI <-> PUIs <-> PCRF binding which are required when an AF (e.g., non-SIP) provides only subscriber identities (no NAI or IMSI information) when contacting the DRA to find the PCRF. Since this issue is applicable to all options it will not be used in the analysis comparison and will be left as an issue to be resolved after the analysis is completed.

Diameter Redirect Agent

According to Diameter Base specification (IETF RFC 3588) the following are requirements of the Diameter Base Redirect agent:

- Redirect agents are by definition protocol transparent and must transparently support the Diameter Base protocol, which includes accounting, and all Diameter applications
- Redirect agents MUST advertise the Relay Application Identifier
- Redirect agents DO NOT relay messages and only return an anwer with the information necessary for Diameter agents to communicate directly
- Redirect agents DO NOT understand/modify application specific messages
- Redirect agents will never receive answer messages
- Redirect agents DO NOT maintain session or transaction states
- Redirect Agents DO NOT support the redirect behaviour required by redirect-DRA as none of the supported Redirect-Host-Usage values mandate that the request resulting in Diameter session termination be sent to the redirect agent.

Diameter Proxy Agent

- Proxy agents that wish to limit resources MUST maintain session state
- Proxy agents MUST maintain transaction states
- Proxy agents MUST understand application-specific messages they wish to support (i.e. by advertising supported applications during capabilities exchange commands)
- Proxy agents can implement policy enforcement, (e.g., for security and load balancing with the network) A derivative of the aforementioned requirement is that Proxy agents can modify contents of an AVP

5.2.5.2.1.8.1 Conclusion on Enhancement to the standard agents:

NOTE: Diameter Base RFC does not preclude configuring an agent to redirect messages of certain types, while acting as relay/proxy agents for other types

[RA]

- Implement application-specific procedures and understand AVPs to create and cache dynamic binding information (i.e. binding of Rx, Gx, Gxa/Gxc session states to a specific PCRF on a per IP-CAN or UE session).

- Implement a DRA-specific redirect behaviour for binding release which needs either a new value for Redirect-Host-Usage (where assignment is by IETF consensus) or a new vendor-specific 3GPP Diameter application.

NOTE 1: The aforementioned requirements implies that enhancements will be also needed on the clients in order to ensure that termination request messages are sent to the redirect DRA

[PA1]

- Needs to keep DRA binding status information (i.e. binding of Rx, Gx, Gxa/Gxc session states to a specific PCRF on a per IP-CAN or UE session)

- A derivative of the above is that the PA must be enhanced in order to determine session termination in Gx using CCR instead of STR

NOTE1: For [PA1] the Realm table and the Peer table of the Diameter client must be configured to ensure that all requests are routed through the DRA.

[PA2]

- Needs to keep DRA binding status information (i.e. binding of Rx, Gx, Gxa/Gxc session states to a specific PCRF on a per IP-CAN or UE session)].

- A derivative of the above is that the PA must be enhanced in order to determine session termination in Gx using CCR instead of STR. As only the first message is transferred by the proxy agent and the following message is not pass the proxy agent, a new mechanism is needed for the proxy agent to inform the client release the binding when the session is terminated.

NOTE 1: The aforementioned requirements implies that enhancements will be also needed on the clients in order to ensure that termination request messages are sent to the proxy DRA

5.2.5.2.1.9 Impacts on existing interfaces

New procedures need to be supported with the Redirect method during roaming and Binding release scenarios for existing interfaces.

Binding Release –

The redirect method does not address the release of binding information upon bearer release as it is not in the direct signaling path. Additional operations will be required for the existing interfaces.

Because the proxy agent will be in the direct signaling path, it can easily remove this information with no additional overhead. In case the client is configured to bypass the proxy DRA for subsequent connections a similar solution to the redirect DRA is required.

Summarizing the changes to different interfaces for each of the candidate solutions:

[RA]

- Client interfaces (Gx, Gxx, S9 and Rx) require re-use of existing messages/procedures to release the Binding at the DRA.

[PA1]

- All messages are proxied through the DRA therefore no impact on the establishment, modification or termination of sessions.

[PA2]

- Only the first establishment message routes via the DRA. Client interfaces (Gxx, S9, and Rx) require re-use of existing messages/procedures to release the Binding at the DRA.

5.2.5.2.1.10 Impacts on clients/servers

The clients have to support the additional redirect functionality as listed in the “Impacts on existing Interfaces” to clear the session binding at the DRA agent.

When the proxy agent is always on the path no changes are required on the client or server. Clients enhancements are necessary when the client is configured to directly communicate with the selected PCRF once the PCRF address is known via the proxy agent.

Summarizing the changes to different interfaces for each of the candidate solutions:

[RA]

- (-) Clients for Gx, Gxx, S9 and Rx require new client logic for Binding Release.

[PA1]

- (+) No changes required on the client and server therefore transparent upgrade.

[PA2]

- (-) Clients for Gxx, S9 and Rx require new client logic for Binding Release.

5.2.5.2.1.11 Interoperability between operators with different DRA solutions

As each administrative domain has a DRA function defined for roaming scenarios, there are no interoperability issues identified between service providers. Typically, the service providers will not want to open their internal topology making the use of redirect alone not practical for roaming scenarios. Therefore, there may be need to proxy the messages between the two networks. If the DRA acts as a proxy, it can achieve both topology hiding as well as PCRF selection for the home realm, for the visited realm, an additional border proxy sitting at the edge of the network is needed, whereas if a DRA is implemented as a redirect agent, there will be a need for both a border proxy sitting at the edge of the home realm and the visited realm.

Editors Note: Use of Security Gateway is an open item and needs to be resolved with SA3 (3GPP TS 33.210)

Summarizing the changes to different interfaces for each of the candidate solutions:

[RA]

- (-) Based on customer need an additional border proxy may be needed to hide the internal IP addresses.

[PA1]

- (+) DRA can provide home topology hiding and therefore no additional components are required. An additional border proxy may be needed to hide the internal IP addresses for the visited realm

[PA2]

(-) Based on customer need an additional border proxy may be needed to hide the internal IP addresses.

5.2.5.2.2 Conclusion

As shown in the above analysis, each DRA approach brings with it some strengths and weaknesses, so, both the redirect and proxy solutions shall be supported for the DRA. On the Diameter client side, it shall be mandatory to support both redirect and proxy approaches. The DRA agent shall also support both the redirect and proxy solutions. Furthermore, the implementation choice between redirect or proxy server shall be based on operator requirements.

5.2.5.3 PCRF selection at attach by the network nodes (non-roaming case)

Diameter Realm-Based Routing (IETF RFC 3588 [8]) is used for routing the Diameter messages from the GW/PCEF or the Non-3GPP Access to the PCRF realm. In this condition, the GW/PCEF or the Non-3GPP Access acts as a Diameter client and the DRA acts as a Diameter agent. In addition, The GW/PCEF or the Non-3GPP Access shall provide the DRA of the PCRF realm with identity parameters upon the first interaction between the access entity and the PCRF realm. The DRA functional entity uses these parameters for ensuring that all Diameter sessions for Gx, S9, Gxa/c and Rx for a certain UE or a certain IP-CAN session established for the UE reach the same PCRF, when multiple and separately addressable PCRFs have been deployed in the Diameter realm.

If the redirect agent is used for DRA, the DRA shall use the redirecting requests procedure as specified in IETF RFC 3588 [8], and include the PCRF address in the Redirect-Host AVP in the Diameter reply sent to the Diameter client.

If the proxy agent is used for DRA, the DRA should use the proxy procedure as specified in IETF RFC 3588 [8]. For PA2 solution (described in clause 5.2.5.2.1), only establishment and termination messages go through the DRA.

The parameters from the GW/PCEF or the Non-3GPP Access may comprise the user identity (UE NAI), APN and UE IP address (3GPP TS 23.203 [6]).

Editor's Note: It is FFS in stage 2 whether other parameters in addition to UE NAI may be used for initial selection of PCRF.

5.2.5.4 PCRF selection by AF

If the AF has the realm identification (i.e. FQDN from a UE NAI) and is located in the home PLMN, the Diameter realm-based routing is used to find the right realm within the operator's network. In this condition, AF acts as the Diameter client, and sends the UE-NAI and PDN information (i.e. APN) if available in a Diameter request to the DRA which acts as a Diameter agent.

Editor's Note: It is FFS how the AF finds the DRA if it does not have the proper knowledge about the UE NAI. It is FFS whether a pre-configured destination realm will suffice in these cases.

Diameter Realm-Based Routing (IETF RFC 3588 [8]) is used for routing the Diameter messages from the AF to the PCRF realm. In addition, the AF shall provide the DRA of the PCRF realm with identity parameters upon the first interaction between the AF and the PCRF realm. The DRA functional entity uses these parameters for ensuring that all Diameter sessions for Gx, S9, Gxa/c and Rx for a certain UE or certain IP-CAN session established for the UE reach the same PCRF, when multiple and separately addressable PCRFs have been deployed in the Diameter realm.

If the redirect agent is used for DRA, the DRA shall use the redirecting requests procedure as specified in IETF RFC 3588 [8], and include the PCRF address in the Redirect-Host AVP in the Diameter reply sent to the AF.

If the proxy agent is used for DRA, the DRA should use the proxy procedure as specified in IETF RFC 3588 [8]. For PA2 solution (described in clause 5.2.5.2.1), only establishment and termination messages go through the DRA.

The parameters from the AF may comprise the UE IP address, PDN and user identity (3GPP TS 23.203 [6]).

Editor's Note: It is FFS in stage 2 whether other parameters in addition to UE NAI may be used for initial selection of PCRF.

5.2.5.5 PCRF selection in a roaming scenario

In the roaming case, a DRA is needed in the visited PLMN when there are more than one PCRF per realm. DRA will ensure that all the related Diameter sessions end up in the same vPCRF for a UE or an IP-CAN session established for the UE.

The S-GW/A-GW in the LBO and home routed cases, the P-GW in the case of LBO and the AF when located in the visited PLMN may use pre-configured information (e.g. based on PDN) to find the visited DRA, and then find the vPCRF. Other possible options are Dynamic peer discovery, or DNS-based

The vPCRF can find the home DRA based on the UE NAI, and then find the hPCRF by the home DRA.

Diameter Realm-Based Routing (IETF RFC 3588 [8]) is used for routing the Diameter messages from the V-PCRF to the H-PCRF realm. In this condition, V-PCRF acts as the Diameter client, the DRA acts as a Diameter agent. In addition, the V-PCRF shall provide the DRA of the H-PCRF realm with identity parameters upon the first interaction

between the V-PCRF and the H-PCRF realm. The DRA functional entity uses these parameters for ensuring that all Diameter sessions for Gx, S9, Gxa/c and Rx for a certain UE or a certain IP-CAN session established for the UEreach the same PCRF, when multiple and separately addressable PCRFs have been deployed in the Diameter realm.

If the redirect agent is used for DRA, the DRA shall use the redirecting requests procedure as specified in IETF RFC 3588 [8], and include the H-PCRF address in the Redirect-Host AVP in the Diameter reply sent to the V-PCRF.

If the proxy agent is used for DRA, the DRA should use the proxy procedure as specified in IETF RFC 3588 [8]. For PA2 solution (described in clause 5.2.5.2.1), only establishment and termination messages go through the DRA.

The parameters from the V-PCRF may comprise the same parameters sent by the GW/PCEF or Non-3GPP Access entity to the V-PCRF, i.e. the user identity (UE NAI), APN and UE IP address (3GPP TS 23.203 [6]).

Editor's Note: It is FFS in stage 2 whether other parameters in addition to UE NAI may be used for initial selection of PCRF.

5.2.5.6 DRA information storage

- The DRA shall maintain PCRF routing information per IP-CAN session or per UE-NAI, depending of the configuration.

  Editor's note: It is FFS how the Diameter clients know this configuration

  DRA has information about user identity (UE NAI), the UE IP address(es),the APN(if available)and the selected PCRF address for a certain IP-CAN Session .

- The PCRF routing information stored for an IP-CAN session in the DRA shall be removed after the IP-CAN session is terminated In case of DRA change (e.g. inter-operator handover),the information about the IP-CAN session stored in the old DRA shall be removed.

- The PCRF routing information stored per UE in the DRA shall be removed when no more IP-CAN and gateway control sessions are active for the UE.

5.3 Protocol impacts

5.3.1 Protocol impacts on S9

5.3.1.1 General

S9 reference point resides between the H-PCRF and V-PCRF. The S9 interface is used for transferring:

1) session information from the V-PCRF to the H-PCRF to support scenarios where both H-PCRF and V-PCRF are employed and the AF resides in the serving network, , e.g. routing optimization with a Local Breakout scenario in the roaming architecture and the Serving Gateway employing a policy enforcement point in the visited network; and

2) policy and charging control information between the H-PCRF and the V-PCRF to support scenarios where both the H-PCRF and the V-PCRF are employed, e.g. routing optimization with a Local Breakout scenario in the roaming architecture and the Serving Gateway employing a policy enforcement point in the visited network.

For the local breakout case, the H-PCRF provisions PCC rules over S9 to the V-PCRF. The latter is required to extract QoS rules and provision them on the BBERF as well as provision PCC rules on the PCEF. As such, the V-PCRF needs to have three separate session contexts: a Gxx session with the BBERF, a Gx session with the PCEF and an S9 session with the H-PCRF. Thus, the Gxx and Gx sessions shall be terminated on the V-PCRF. The V-PCRF shall initiate an S9 session with the H-PCRF.

For the local breakout case, when the AF is in the visited PLMN, Rx messages are forwarded over S9 to the H-PCRF, and as such, the S9 procedures shall encompass all of the Rx procedures. The V-PCRF forwards as well PCC rules request from the PCEF received over Gx and provisions PCC rules over Gx on the PCEF. As such, S9 commands need to encompass Gx commands. In this case, the V-PCRF shall send the PDN information if available to the H-PCRF to indicate the PDN the user is connected to, which may be used by the H-PCRF to perform session binding.

Editor's note: It is FFS how the AF gets the PDN information and sends to the PCRF.

For Local Breakout scenario, in order to carry out online charging accurately in the H-PLMN, the Diameter identities of the OCS in the H-PLMN may be passed in the re-used Charging-Information AVP once per IP-CAN session from the H-PCRF to the V-PCRF and then be forwarded to the PCEF in the V-PLMN. The Diameter identities of the OCS or the proxy OCS in the V-PLMN may also be passed once per IP-CAN session from the V-PCRF to the PCEF along with the Diameter identities of the OCS in the H-PLMN.

Editor's note: The Allocation-and-Retention-Priority AVP, as specified for the Gx reference point, shall be included in the S9 reference point.

Editor's note: Whether for Local Breakout scenario an OCS proxy is required for the Gy interface is FFS.

5.3.1.1.1 H-PCRF discovery over S9

The V-PCRF shall provide the DRA of the H-PCRF realm with user identity parameters upon the first interaction between the V-PCRF and the H-PCRF realm. The DRA uses these parameters for ensuring that all Diameter sessions for Gx, S9, Gxa/c and Rx for a certain UE or a certain IP-CAN session established for the UE reach the same PCRF, when multiple and separately addressable PCRFs have been deployed in the Diameter realm.

The parameters from the V-PCRF may comprise the same parameters sent by the GW/PCEF or Non-3GPP Access entity to the V-PCRF, i.e. the user identity (UE NAI), APN and UE IP address (3GPP TS 23.203 [6]).

Editor's Note: It is FFS in stage 2 whether other parameters in addition to UE NAI may be used for initial selection of PCRF.

The UE IP address, the APN and the user identity (UE NAI) can be transferred through the S9 interface as per the current Gx specification, i.e. using the Framed-IP-Address AVP or Framed-IPv6-Prefix AVP, the Called-Station-ID AVP and the Subscription-ID AVP, respectively.

5.3.1.2 Commands

The S9 procedures for home-routed traffic can be mapped to the Gxa and Gxc procedures using the same command codes and corresponding AVPs.

- The procedure Gateway Control Session Establishment/Ack is mapped to the CCR and CCA command codes. On reception of the CCR command with CC-Request-Type AVP set to the value "INITIAL_REQUEST" the V-PCRF shall store the session information provided in the request including the MN-NAI to be used in subsequent messages within the same Gateway Control Session and shall forward the CCR request to the H-PCRF. On reception of a successful CCA command, the V-PCRF shall the CCA command to the S-GW/A-GW.

- The procedure Gateway Control Session Termination/Ack is mapped to the CCR and CCA command codes. V-PCRF shall forward the CCR command with CC-Request-Type AVP set to the value "TERMINATION_REQUEST" to the H-PCRF. On receipt of a successful CCA command, the V-PCRF shall remove the session information stored for that Gateway Control Session and shall send the CCA command to the S-GW/A-GW.

- The procedure Gateway Control and QoS Rules Request/Response is mapped to the CCR and CCA command codes. If the H-PCRF sends the Gateway Control and QoS Rules Response towards the S-GW/A-GW, the V-PCRF shall validate the contents of the QoS-Information AVP received within the PCC Rules. If the QoS validation fails the V-PCRF shall send a CCR command to the H-PCRF including the Charging-Rule-Report AVP to indicate the PCC Rules that were not accepted, the Event-Trigger AVP to indicate 'UNSUCCESSFUL-QoS-VALIDATION' and the QoS-Information AVP to indicate the acceptable QoS. The V-PCRF installs the corresponding QoS rules at the S-GW/A-GW.

- The procedure Policy and Charging Rule provision/ack is mapped to the RAR and RAA command codes. If the H-PCRF sends the Policy and Charging Rule provisioning towards the S-GW/A-GW, the V-PCRF shall validate the QoS information received with the PCC Rules. If the QoS validation fails the V-PCRF shall reject the request using a RAA command to the H-PCRF including the Charging-Rule-Report AVP to indicate the PCC Rules that were not accepted, the Event-Trigger AVP to indicate 'UNSUCCESSFUL-QoS-VALIDATION' and the QoS-Information AVP to indicate the acceptable QoS.

For the home routed traffic case, PCC Rules sent over S9 do not include charging information.

The S9 procedures for Visited Access:

- The Application Session info is mapped to the AAR and AAA command codes. If the AF sends the session information to the V-PCRF, the V-PCRF sends the AAR towards the H-PCRF to provide the session information. The H-PCRF performs session binding as described in 3GPP TS 29.213 [xx]. If the H-PCRF fails in executing the session binding, the H-PCRF responds to the AF with the Experimental-Result-Code AVP set to the value IP_CAN_SESSION_NOT_AVAILABLE in the AAA command via the V-PCRF. The H-PCRF initiates the procedure Policy and Charging Rule provision/ack mapped to the AAA command code.

Editors note:– FFS whether PCC rules are provisioned including the AAA message.

- The procedure Gateway Control Session Termination/Ack is mapped to CCR and CCA command codes. V-PCRF shall terminate the Rx session according to 3GPP TS 29.214[yy]. On receipt of a successful ASA from the AF and CCA command from the H-PCRF, the V-PCRF shall remove the session information stored for that Gateway Control Session and shall send the CCA command to the AN-GW/PDN-GW.

- The procedure AF Session Termination occurs as defined in 3GPP TS 29.214[yy], the V-PCRF shall send a RAR command with the Charging-Rule-Remove AVP to the AN-GW/PDN-GW. On receipt of a successful RAA command, the V-PCRF shall the command to the H-PCRF. On receipt of a successful command from the H-PCRF, the V-PCRF shall remove the session information stored for that Gateway Control Session and respond with the successful STA to the AF.

5.3.1.3 AVPs

CCR/CCA and RAR/RAA commands will include information elements used in Gx, Gxa and Gxc depending on the access network that the UE is attached to. These information elements are listed in clauses 5.3.3.2 and 5.3.3.4.

In addition specific AVPs needed for S9 interface are listed in this clause.

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

The Charging-Rule-Report AVP (AVP code 1018) is of types Grouped, and it is used to report the status of PCC rules. The Charging-Rule-Report AVP is used to report the status of the PCC rules that are not acceptable by the V-PCRF.

AVP Format:

```
Charging-Rule-Report ::= < AVP Header: 1018 >
                         *[Charging-Rule-Name]
                         *[Charging-Rule-Base-Name]
                          [PCC-Rule-Status]
                          [QoS-Information]
                         *[AVP]
```

5.3.1.3.2 Event-Trigger AVP (All access types)

The Event-Trigger AVP (AVP code 1006) is of type Enumerated.

When sent from the H-PCRF to the V-PCRF, the Event-Trigger AVP indicates an event that shall cause a re-request of PCC rules. When sent from the V-PCRF to the H-PCRF the Event-Trigger AVP indicates that the corresponding event has occurred at the V-PCRF.

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

The following values are defined:

UNSUCCESSFUL-QoS-VALIDATION (X)

This value shall be used in a CCR or RAA command to indicate that the V-PCRF has validated the requested QoS e.g. against the defined QoS profile per PLMN. The validation has failed.

5.3.1.4 Diameter Application

As the V-PCRF needs to initiate an S9 session with the H-PCRF, it needs to choose one application id to use when communicating with the H-PCRF. As such, the following options are possible regarding the S9 application id:

- A new application-id is used for S9
- S9 re-uses the Gx application id. This option is only valid if the Gx application encompasses all of the additional AVPs and commands that are needed by Gxa/c and, if the AF is in the V-PLMN, Rx messages are forwarded by the V-PCRF to the H-PCRF.

NOTE: The S9 reference point will encompass Rx messages forwarded from the V-PCRF to the H-PCRF when the AF is in the V-PLMN. However, this is not the case for the S9 Diameter application.

Editor's note: It is FFS whether Gxx messages will be forwarded over the S9 reference point.

Editor's note: If the AF is in the V-PLMN, it is FFS whether the Rx messages will be forwarded from the V-PCRF to the H-PCRF over the S9 reference point or if the Rx information will be encompassed in S9 messages, in which case, an S9 Diameter application would be required with a new application id.

Editor's note: A further study as to the S9 requirements is required before one of the two options can be selected.

5.3.2 Protocol impacts on Rx

5.3.2.1 General

The operator's services providing service information over Rx to the PCRF is supported.

5.3.2.1.1 PCRF discovery over Rx

The AF shall provide the DRA of the PCRF realm with user identity parameters upon the first interaction between the AF and the PCRF realm. The DRA uses these parameters for ensuring that all Diameter sessions for Gx, S9, Gxa/c and Rx for a certain IP-CAN session reach the same PCRF, when multiple and separately addressable PCRFs have been deployed in the Diameter realm. The parameters from the AF may comprise the UE IP address, PDN and user identity (3GPP TS 23.203 [6]).

The AF may have access to a user's public user identity and private user identity, i.e. the AF may provide the user identity in various formats.

Editor's Note: It is FFS what to do if the AF does not have access to a user's public user identity and private user identity.

The public user identity is of the form of either a SIP uniform resource identifier (URI) or of a telephone uniform resource locator (tel URI). If there is no ISIM application to host the public user identity, a temporary public user identity shall be derived, based on the IMSI. The private user identity shall take the form of an NAI, and shall have the form username@realm. If the private user identity is not known, the private user identity shall be derived from the IMSI. (Refer to 3GPP TS 23.003 [8] and IETF RFC 3261 [10]). IMSI comprises maximum 15 digits consisting of Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Subscriber Identification Number (MSIN),

Editor's Note: It is FFS in stage 2 whether other parameters in addition to UE NAI may be used for initial selection of PCRF.

The parameters can be transferred through the Rx interface as per the current Rx specification, i.e. using the Framed-IP-Address AVP or Framed-IPv6-Prefix AVP for UE IP address, and using the Subscription-ID AVP for the user identity (UE NAI).

Editor's Note: It is FFS whether information about APN shall be transferred through the Rx interface.

5.3.2.2 Commands

5.3.2.2.1 AA-Answer (AAA) command

The AAA command is revised from rel-7 Rx.

The modifications from Rx rel-7 are:

- Deprecated 3GPP-RAT-Type and replaced with a generic RAT-Type AVP that is applicable to all radio access technologies.

Message Format:

```
<AA-Answer> ::=  < Diameter Header: 265, PXY >
                 < Session-Id >
                 { Auth-Application-Id }
                 { Origin-Host }
                 { Origin-Realm }
                 [ Result-Code ]
                 [ Experimental-Result ]
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                 [ Acceptable-Service-Info ]
                 [ IP-CAN-Type ]
                 [ RAT-Type ]
                *[ Event-Trigger ]
                *[ Charging-Rule-Remove ]
                *[ Charging-Rule-Install ]
                *[ QoS-Information ]
                 [ Error-Message ]
                 [ Error-Reporting-Host ]
                *[ Failed-AVP ]
                 [ Origin-State-Id ]
                *[ Redirect-Host ]
                 [ Redirect-Host-Usage ]
                 [ Redirect-Max-Cache-Time ]
                *[ Proxy-Info ]
                *[ AVP ]
```

Editor's Note: It is FFS which messages will be used to provision the PCC rules over the S9 interface.

5.2.3.2.2 Re-Auth-Request (RAR) command

The RAR command is revised from rel-7 Rx.

The modifications from Rx rel-7 are:

- Deprecated 3GPP-RAT-Type and replaced with a generic RAT-Type AVP that is applicable to all radio access technologies.

Message Format:

```
<RA-Request> ::= < Diameter Header: 258, REQ, PXY >
                 < Session-Id >
                 { Origin-Host }
                 { Origin-Realm }
                 { Destination-Realm }
                 { Destination-Host }
                 { Auth-Application-Id }
                 { Specific-Action }
                *[ Access-Network-Charging-Identifier ]
                 [ Access-Network-Charging-Address ]
                *[ Flows ]
                *[ Subscription-ID ]
                 [ Abort-Cause ]
                 [ IP-CAN-Type ]
                 [ RAT-Type ]
                 [ Origin-State-Id ]
```

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

5.3.3 Protocol impacts on Gx Gxa, Gxb, Gxc

5.3.3.1 General

The Gx protocol is based on Gx and incorporates the needs specified in TS 23.401, TS 23.402 and TS 23.203.

There are four different variants defined for the Gx interface: Gx, Gxa, Gxb, Gxc. The Gxa and Gxc interfaces should be as similar as possible and shall be based on the Gx interface.

NOTE: The Gxb interface is not specified in this release

Editor's note: It is FFS whether Gxa and Gxc need to have different application identifiers.

The service level (per SDF) QoS parameters are conveyed in PCC rules (one PCC rule per SDF) over the Gx reference point. The service level QoS parameters consist of a QoS Class Identifier (QCI) Allocation and Retention Priority (ARP) and authorised Guaranteed and Maximum Bit Rate values for uplink and downlink.

NOTE 1: For E-UTRAN, the value of the ARP of an EPS bearer is identical to the value of the ARP of the SDF(s) mapped to that EPS bearer.

NOTE 2: The bearer level QCI of an EPS bearer is identical to the value of the QCI of the SDF(s) mapped to that EPS bearer.

5.3.3.1.1 Allocation and Retention Priority (ARP)

The following service level QoS parameters are conveyed in PCC rules from the PCRF to the PCEF:

- QoS Class Identifier (QCI),
- Allocation and Retention Priority (ARP),
- Guaranteed Bit Rate Uplink (GBR uplink),
- Guaranteed Bit Rate Downlink (GBR downlink),
- Maximum Bit Rate Uplink (MBR uplink),
- Maximum Bit Rate Downlink (MBR downlink).

ARP is a new parameter compared to the Rel-7 PCC (refer to 3GPP TS 23.401 [2]).

The primary purpose of ARP is to decide whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations. In addition, the ARP can be used to decide which bearer(s) to drop during exceptional resource limitations.

The service level ARP assigned by PCRF in a PCC rule may be different from the bearer level ARP stored in subscription data. For E-UTRAN the value of the ARP of an EPS bearer is identical to the value of the ARP of the SDF(s) mapped to that EPS bearer.

Editor's note: It is open, how the PCRF is supposed to derive the values for the service level ARP.

The PCRF sends the ARP to the PCEF with the other service level QoS parameters in the QoS-Information AVP. The QoS-Information AVP shall be revised accordingly.

5.3.3.1.2 PCRF discovery over Gx, Gxa and Gxc

The GW/PCEF or the Non-3GPP Access shall provide the DRA of the PCRF realm with user identity parameters upon the first interaction between the access entity and the PCRF realm. The DRA uses these parameters for ensuring that all Diameter sessions for Gx, S9, Gxa/c and Rx for a certain IP-CAN session reach the same PCRF, when multiple and separately addressable PCRFs have been deployed in the Diameter realm. The parameters from the GW/PCEF or the Non-3GPP Access may comprise the user identity (UE NAI), APN and UE IP address (3GPP TS 23.203 [6]).

The GW/PCEF or the Non-3GPP Access may provide the user identity in various formats. In the GTP variant the initial bearer establishment contains IMSI as a user identity (3GPP TS 29.060 [5]) which comprises maximum 15 digits consisting of Mobile Country Code (MCC), Mobile Network Code (MNC) and Mobile Subscriber Identification Number (MSIN), (3GPP TS 23.003 [8]). Other accesses may provide user identity as a NAI which is of format "*username@realm*" and may be 72 octets long (IETF RFC 2486 [9]).

Editor's Note: It is FFS in stage 2 whether other parameters in addition to UE NAI may be used for initial selection of PCRF.

The UE IP address, the APN and the user identity (UE NAI) can be transferred through the Gx and Gxa/c interfaces as per the current Gx specification, i.e. using the Framed-IP-Address AVP or Framed-IPv6-Prefix AVP, the Called-Station-ID AVP and the Subscription-ID AVP, respectively.

5.3.3.1.3 Care-of-Address (CoA)

When UE attaches to the trusted non-3GPP access and DSMIPv6 is used, an IP address or an IPv6 prefix is assigned to the UE by the trusted non-3GPP access system. This IPv4 address or an IPv6 address belonging to the assigned IPv6 prefix will be used as a Care-of-Address for DSMIPv6 over the S2c reference point. This address information is included in Gateway Control Session Establishment message and Indication of IP-CAN Session Establishment message. It shall also be included in indication of IP-CAN session modification message when the CoA changes (e.g. handover in S2c case).

Over the Gxa gateway control session, the CoA information is transferred from the BBERF to the PCRF using the Framed-IP-Address AVP or Framed-IPv6-Prefix AVP.

Over the Gx session, the HoA is transferred from the PCEF to the PCRF through using the Framed-IP-Address AVP or Framed-IPv6-Prefix AVP. The CoA is transferred from the PCEF to the PCRF using the CoA-IP-Address AVP or CoA-IPv6-Address AVP.

Editor's Note: In IPv6 case, whether the CoA IPv6 address, instead of the IPv6 prefix, can be sent over the Gxa session is FFS.

5.3.3.2 Commands

5.3.3.2.1 CC-Request (CCR) Command

The CCR command is revised from the rel-7 Gx.

The modifications from Gx rel-7 are:

- Deprecated 3GPP-RAT-Type and replaced with a generic RAT-Type AVP that is applicable to all radio access technologies.

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 ]
                 [ Bearer-Control-Mode ]
                 [ 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 ]
[ 3GPP-SGSN-MCC-MNC ]
[ 3GPP-SGSN-Address ]
[ 3GPP-SGSN-IPv6-Address ]
[ RAI ]
[ 3GPP-User-Location-Info]
[ Called-Station-ID ]
[ Bearer-Usage ]
[ Online ]
[ Offline ]
*[ TFT-Packet-Filter-Information ]
*[ Charging-Rule-Report]
*[ Event-Trigger]
 [ Access-Network-Charging-Address ]
*[ Access-Network-Charging-Identifier-Gx ]
*[ Proxy-Info ]
*[ Route-Record ]
*[ AVP ]
```

5.3.3.3 AVPs

5.3.3.3.1. QoS-Information AVP

AVP Format (Rel-7 AVP revised with Allocation-and-Retention-Priority):

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

5.3.3.3.2 Allocation-and-Retention-Priority AVP

The Allocation-and-Retention-Priority AVP (AVP code xxxx) is of type Enumerated. The AVP is sent from the PCRF to the PCEF. The AVP indicates a priority for deciding whether a bearer establishment or modification request can be accepted or needs to be rejected in case of resource limitations, or which bearer(s) to drop during exceptional resource limitations.

Editor's note: The following values are defined for 3GPP access types E-UTRAN, UTRAN and GERAN (refer to 3GPP TS 23.107 [4] and 29.060 [5]): 1, 2 and 3. It is open whether new values will be defined for SAE accesses within Rel-8.

5.3.3.3.3 Access-Node-MCC-MNC AVP (All access types)

The Access-Node-MCC-MNC AVP (AVP code xxxx) is of type UTF8String, and it indicates the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the gateway (S-GW for 3GPP access and A-GW for trusted non-3GPP access). The format of the UTF8String value is the MCC immediately followed by the MNC. The MCC shall be 3 digits and the MNC shall be either 2 or 3 digits. There shall be no padding characters between the MCC and MNC.

Editor's Note: The AVP may be renamed

5.3.3.3.4 TFT-Filter AVP

The TFT-Filter AVP (AVP code 1012) definition is revised from rel-7 Gx [12]. The restrictions on the direction and value of the destination address have been relaxed.

Below is the new definition:

The TFT-Filter AVP (AVP code 1012) is of type IPFilterRule, and it defines the TFT packet filter with the following information:

- Direction (in or out)

- Protocol
- Source IP address (possibly masked) or “assigned”.
- Source port (single value, list or ranges or may be omitted to indicate that any port is allowed)
- Destination IP address (possibly masked) or “assigned”.
- Destination port (single value, list or ranges or may be omitted to indicate that any port is allowed)

The IPFilterRule type shall be used with the following restrictions:

- Action shall be set to "permit".
- No options shall 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.

The keyword “assigned” shall mean the IP address of the UE as indicated by the GW/PCEF in the Framed-IP-Address and Framed-IPv6-Prefix AVPs.

Editor’s note: It is FFS whether the keyword “assigned” will be allowed in this AVP.

5.3.3.3.5 RAT-Type AVP

The RAT-Type AVP (AVP code yyyy) 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. Refer to 29.060 [5].

GERAN (1001)

This value shall be used to indicate that the RAT is GERAN. Refer to 29.060 [5].

GAN (1002)

This value shall be used to indicate that the RAT is GAN. Refer to 29.060 [5].

HSPA_EVOLUTION (1003)

This value shall be used to indicate that the RAT is HSPA Evolution. Refer to 29.060 [5].\

CDMA2000_1X (2000)

This value shall be used to indicate that the RAT is CDMA2000 1X. Refer to [13].

HRPD (2001)

This value shall be used to indicate that the RAT is HRPD. Refer to [13].

UMB (2002)

This value shall be used to indicate that the RAT is UMB. Refer to [13].

5.3.3.3.6 CoA-IP-Address AVP

The CoA-IP-Address AVP (AVP Code xxx) is of type Octetstring and contains the mobile node's IPv4 care-of-address.

5.3.3.3.7 CoA-IPv6-Address AVP

The CoA-IPv6-Address AVP (AVP Code xxx) is of type Octetstring and contains the mobile node's IPv6 care-of-address.

Editor's Note: It is for FFS how the above two AVPs are used within the relevant Diameter commands.

5.3.3.3.8 Tunnel-Information AVP

The Tunnel-Information AVP (AVP code ????) 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 shall include a Tunnel-Header-Length AVP, which provides the length of the tunnel header and identifies the offset where the inner header starts. 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-Information AVP may also include a Tunnel-Header-Filter AVP to identify the tunnel (outer) header information, which includes information such as the Home Agent IPv6 address and the Home Agent IPv4 address.

AVP Format:

```
Tunnel-Information ::= < AVP Header: ???? >
                           { Tunnel-Header-Length }
                           *[ Tunnel-Header-Filter ]
```

5.3.3.3.9 Tunnel-Header-Length AVP

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

5.3.3.3.10 Tunnel-Header-Filter AVP

The Tunnel-Header-Filter AVP (AVP code ????) is of type IPFilterRule, and it defines the tunnel (outer) header filter information of a tunnelled IP flow.

The Tunnel-Header-Filter AVP includes the following information:

- Direction (in or out)
- Protocol
- Source IP address (possibly masked).
- Source port (single value, list or ranges or may be omitted to indicate that any port is allowed)
- Destination IP address (possibly masked).
- Destination port (single value, list or ranges or may be omitted to indicate that any port is allowed)

The IPFilterRule type shall be used with the following restrictions:

- Action shall be set to "permit".
- No options shall 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.

Editor's Note: It is for FFS how the above three AVPs are used within the relevant Diameter commands.

Editor's Note: Whether other information, in addition to home agent address(es), is needed is FFS.

5.3.3.4 Gxa protocoldelta

5.3.3.4.1 Commands

CCR/CCA commands will be used for the operations received from the Trusted non-3GPP access network towards the PCRF, in order to create, modify or terminate the Gateway Control session.

RAR/RAA commands will be used for the operations received from the PCRF towards the Trusted non-3GPP access network in order to provide PCC rules and/or Event Triggers to the Access Gateway.

5.3.3.4.2 AVPs

5.3.3.4.2.1 General

The following table shows the protocol delta for AVPs with regards to current Gx interface as specified in Release 7 3GPP TS 29.212 [12]

Table 5.3.3.4.2.1: Gxa Diameter AVPs

Attribute Name	Applicability	Comments
Access-Network-Charging-Identifier-Gx	Not applicable	
Bearer-Control-Mode	Not applicable	
Bearer-Identifier	FFS	It is FFS whether this identifier is required for the non-3GPP access.
Bearer-Operation	FFS	An indication to indicate resource initiation, modification or termination is required. It is FFS if this AVP will be used for that purpose.
Bearer-Usage	FFS	It is FFS whether the bearer concept can apply during the GW-control session establishment.
Charging-Rule-Install	Applicable	AVP re-naming should be considered (e.g. PCC-Rule-Install)
Charging-Rule-Remove	Applicable	AVP re-naming should be considered
Charging-Rule-Definition	Applicable	It is FFS whether this AVP will include Max-Requested-Bandwidth-UL & Max-Requested-Bandwidth-DL AVP when the PCC rule does not contain Guaranteed-Bandwidth-UL & Guaranteed-Bandwidth-DL AVP information. This AVP will not include charging related information (Service-Identifier, Rating-Group, Reporting-Level, On-line, Off-line, Metering-Method, AF-charging-identifier) nor gating information (Flow-Status) AVP re-naming should be considered
Charging-Rule-Base-Name	Applicable	AVP re-naming should be considered
Charging-Rule-Name	Applicable	AVP re-naming should be considered
Charging-Rule-Report	Applicable	AVP re-naming should be considered
Event-Trigger	Applicable	Specific 2G/3G Event triggers (e.g. SGSN change) will not be subscribed and triggered.
IP-CAN-Type	Applicable	Specific IP-CAN Type required
Guaranteed-Bitrate-DL	Applicable	
Guaranteed-Bitrate-UL	Applicable	
Metering-Method	Not applicable	
Network-Request-Support	Not applicable	
Offline	Not applicable	
Online	Not applicable	
Precedence	Applicable	
Reporting-Level	Not applicable	
PCC-Rule-Status	Applicable	
QoS-Class-Identifier	Applicable	
QoS_Information	Applicable	This AVP will not be provided during the GW Control Session Establishment. This AVP is not applicable at command level.
TFT-Filter	Applicable	
TFT-Packet-Filter-Information	Applicable	
ToS-Traffic-Class	Applicable	
A-GW Address (New)	Applicable	New AVP to provide the Access Gateway Address. (both MCC+MNC and IP address may be available)
3GPP-RAT-Type	Not Applicable	Deprecated
RAT-Type (New)	Applicable	A generic RAT type is required to include all radio access types.
3GPP-SGSN-Address	Not applicable	
3GPP-SGSN-IPv6-Address	Not applicable	
3GPP-User-Location-Info	Not applicable	
Access-Network-Charging-Address	Not applicable	
Access-Network-Charging-Identifier-Value	Not applicable	
AF-Charging-Identifier	Not applicable	
Called-Station-ID	Applicable	
CC-Request-Number	Applicable	
CC-Request-Type	Applicable	
Charging-Information	Not applicable	
Flow-Description	Applicable	
Flows	Not Applicable	
Flow-Status	Applicable	
Framed-IP-Address	Applicable	
Framed-IPv6-Prefix	Applicable	
Max-Requested-Bandwidth-UL	Applicable	

Max-Requested-Bandwidth-DL	Applicable	
RAI	Not applicable	
Rating-Group	Not applicable	
Service-Identifier	Not applicable	
Subscription-Id	Applicable	
User-Equipment-Info	Applicable	

5.3.3.4.2.2 Definition of new AVPs

5.3.3.4.2.2.1 Access-Node-MCC-MNC AVP (All access types)

When used over Gxa such AVP indicates the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the A-GW function for the trusted non-3GPP access. The format of this AVP is defined in clause 5.3.3.3.x.

5.3.3.5 Gxb protocoldelta

The details associated with the Gxb reference point are not specified in this release

5.3.3.6 Gxc protocoldelta

5.3.3.6.1 Commands

CCR/CCA commands will be used for the operations received from the Serving GW towards the PCRF, in order to create, modify or terminate the Gateway Control session.

RAR/RAA commands will be used for the operations initiated by the PCRF towards the Serving GW, in order to provide PCC rules and/or Event Triggers.

5.3.3.6.2 AVPs

5.3.3.6.2.1 General

The following table shows the protocol delta for AVPs with regards to current Gx interface as specified in Release 7 3GPP TS 29.212 [12]

Table 5.3.3.6.2.1: Gxc Diameter AVPs

Attribute Name	Applicability	Comments
Access-Network-Charging-Identifier-Gx	Not applicable	
Bearer-Control-Mode	FFS	See Note 1.
Bearer-Identifier	FFS	See Note 1
Bearer-Operation	Applicable	See Note 1
Bearer-Usage	Applicable	See Note 1
Charging-Rule-Install	Applicable	AVP re-naming should be considered
Charging-Rule-Remove	Applicable	AVP re-naming should be considered
Charging-Rule-Definition	Applicable	It is FFS whether this AVP will include Max-Requested-Bandwidth-UL & Max-Requested-Bandwidth-DL AVP when the PCC rule does not contain Guaranteed-Bandwidth-UL & Guaranteed-Bandwidth-DL AVP information. This AVP will not include charging related information (Service-Identifier, Rating-Group, Reporting-Level, On-line, Off-line, Metering-Method, AF-charging-identifier) nor gating information (Flow-Status) AVP re-naming should be considered
Charging-Rule-Base-Name	Applicable	AVP re-naming should be considered
Charging-Rule-Name	Applicable	AVP re-naming should be considered
Charging-Rule-Report	Applicable	AVP re-naming should be considered
Event-Trigger	Applicable	
IP-CAN-Type	Applicable	Specific IP-CAN Types required
Guaranteed-Bitrate-DL	Applicable	
Guaranteed-Bitrate-UL	Applicable	
Metering-Method	Not Applicable	
Network-Request-Support	Not Applicable	
Offline	Not Applicable	
Online	Not Applicable	
Precedence	Applicable	
Reporting-Level	Not Applicable	
PCC-Rule-Status	Applicable	
QoS-Class-Identifier	Applicable	
QoS_Information	Applicable	QoS-Information AVP when included at command level will include a new AVP called AMBR during the GW control session establishment. AMBR may also be included during the GW control session modification. Max-Requested-Bandwidth-UL & Max-Requested-Bandwidth-DL AVP within QoS-Information AVP will not be sent during the Gw control session establishment.
TFT-Filter	Applicable	
TFT-Packet-Filter-Information	Applicable	
ToS-Traffic-Class	Applicable	
S-GW Address (New)	Applicable	New AVP to provide the Serving Gateway Address
AMBR (New)		New AVP to include the Accumulated Maximum Bitrate
3GPP-RAT-Type	Not Applicable	Deprecated and replaced by a more generic RAT-Type.
RAT-Type (New)		Generic RAT type
3GPP-SGSN-Address	Applicable	
3GPP-SGSN-IPv6-Address	Applicable	
3GPP-SGSN-MCC-MNC	Applicable	
3GPP-User-Location-Info	Applicable	
Access-Network-Charging-Address	Not Applicable	
Access-Network-Charging-Identifier-Value	Not Applicable	
AF-Charging-Identifier	Not Applicable	
Called-Station-ID	Applicable	
CC-Request-Number	Applicable	

CC-Request-Type	Applicable	
Charging-Information	Not Applicable	
Flow-Description	Applicable	
Flows	Not Applicable	
Flow-Status	Applicable	
Framed-IP-Address	Applicable	This AVP may be provided together with Framed-IPv6-Prefix AVP
Framed-IPv6-Prefix	Applicable	This AVP may be provided together with Framed-IP-Address AVP
Max-Requested-Bandwidth-UL	Applicable	
Max-Requested-Bandwidth-DL	Applicable	
RAI	Applicable	
Rating-Group	Not Applicable	
Service-Identifier	Not Applicable	
Subscription-Id	Applicable	
User-Equipment-Info	Applicable	

Note 1: It is FFS whether currently defined bearer related AVPs 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 AVP for 2G/3G accesses..

5.3.3.6.2.2 Definition of new AVPs

5.3.3.6.2.2.1 Access-Node-MCC-MNC AVP (All access types)

When used over Gxc such AVP indicates the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the S-GW. The format of this AVP is defined in clause 5.3.3.3.x.

Editor's Note It is FFS if different AVPs are required to convey the MCC-MNC values on the Gxc interfaces to address the scenario where a trusted non-3GPP system is anchored via the S-GW. In such a case, both A-GW and S-GW MCC-MNC values may need to be conveyed over Gxc.

5.3.3.7 Diameter Application

A major difference between Gx and Gxc, and Gx and Gxa, is that Gx supports policy and charging control, i.e. PCCRules, whereas Gxc and Gxa support only policy/QoS control, i.e. QoS rules. QoS Rules (and Event Triggers) are sent from the PCRF to the BBERF (or to Trusted Non-3GPP Access) upon a gateway control session establishment or upon a later modification. PCC rules (and Event Triggers) are sent from the PCRF to the PDN-GW upon the IP-CAN session establishment or upon a later modification, refer to 3GPP TS 23.402 [3]. This means there are two possibilities for the Diameter application for the Gx variants (refer to 3GPP TR 29.909 [14]):

- Using an own Diameter application for Gx and an own application jointly for Gxa and Gxc means that the Diameter entities at the BBERF and at the Trusted Non-3GPP Access shall understand only the required (QoS Rules and Event Trigger related) subset of the parameters/AVPs of Gx.

- Using the same Diameter application (i.e. the same Diameter application ID) for Gx, Gxa and Gxc means that the Diameter entities at the BBERF and at the Trusted Non-3GPP Access shall understand also the charging related parameters/AVPs which they actually don't need and don't use.

Editor's note: Stage 2 requirements are not yet mature, with place holders in stage 2 specifications (TS 23.203). Decision on the two possibilities above is open.

5.4 QoS Mapping for Trusted Non-3GPP IP-CANs

5.4.1 Authorized IP QoS parameters to Authorized access network QoS parameters mapping in PCEF or BBERF

Editor's Note: This clause will contain detailed rules on how to map authorized IP QoS parameters to authorized access network QoS parameters

5.4.2 QoS parameter mapping in the UE for trusted non-3GPP IP-CANs

If the UE uses a different QoS mapping mechanism then this clause does not apply.

5.4.2.1 Framework for QoS mapping in the UE

Editor's Note: This section will define the framework for QoS mapping in the UE.

5.4.2.2 SDP parameters to SDF QoS parameters mapping in UE

Table 5.4.2.2.1: Rules for derivation of the Maximum Authorized Bandwidth DL/UL and the Maximum Authorized QoS Class Identifier per flow identifier in the UE

Authorized QoS Parameter per flow identifier	Derivation from SDP Parameters (see NOTE 4)
Maximum Authorized Bandwidth DL (Max_BW_DL) and UL (Max_BW_UL) per flow identifier (see NOTE 5)	

```
/* The Direction of the IP flow(s) identified by the flow identifier */

IF a=recvonly THEN
      IF <SDP direction> = mobile originated THEN
            Direction:= downlink;
      ELSE /* mobile terminated */
            Direction:= uplink;
      ENDIF;
ELSE;
      IF a=sendonly THEN
            IF <SDP direction> = mobile originated THEN
                  Direction: = uplink;
            ELSE /* mobile terminated */
                  Direction:= downlink;
            ENDIF;
      ELSE /*sendrecv, inactive or no direction attribute*/
            Direction:=both;
      ENDIF;
ENDIF;

/* Max_BW_UL and Max_BW_DL */

IF media IP flow(s) THEN
   IF b_AS=AS:<bandwidth> is present THEN
      IF Direction=downlink THEN
         Max_BW_UL:= 0;
         Max_BW_DL:= b_AS;
      ELSE
         IF Direction=uplink THEN
            Max_BW_UL:= b_AS;
            Max_BW_DL:= 0;
         ELSE /*Direction=both*/
            Max_BW_UL:= b_AS;
            Max_BW_DL:= b_AS;
         ENDIF;
      ENDIF;
   ELSE
      bw:= as set by the UE manufacturer;
      IF Direction=downlink THEN
         Max_BW_UL:= 0;
         Max_BW_DL:= bw;
      ELSE
         IF Direction=uplink THEN
            Max_BW_UL:= bw;
            Max_BW_DL:= 0;
         ELSE /*Direction=both*/
            Max_BW_UL:= bw;
            Max_BW_DL:= bw;
         ENDIF;
      ENDIF;
   ENDIF;
ELSE /* RTCP IP flow(s) */
   IF b_RS=RS:<bandwidth> and b_RR=RR:<bandwidth> is present THEN
      Max_BW_UL:= (b_RS + b_RR) / 1000;
      Max_BW_DL:= (b_RS + b_RR) / 1000;
   ELSE
      IF b_AS=AS:<bandwidth> is present THEN
         IF b_RS=RS:<bandwidth> is present and b_RR=RR:<bandwidth> is not
present THEN
            Max_BW_UL:= MAX[0.05 * b_AS, b_RS / 1000];
            Max_BW_DL:= MAX[0.05 * b_AS, b_RS / 1000];
         ENDIF;
         IF b_RS=RS:<bandwidth> is not present and b_RR=RR:<bandwidth> is
present THEN
            Max_BW_UL:= MAX[0.05 * b_AS, b_RR / 1000];
            Max_BW_DL:= MAX[0.05 * b_AS, b_RR / 1000];
```

Authorized QoS Parameter per flow identifier	Derivation from SDP Parameters (see NOTE 4)

	ENDIF;
	IF b_{RS}=RS:<bandwidth> and b_{RR}=RR:<bandwidth> is not present THEN
	Max_BW_UL:= 0.05 * b_{AS};
	Max_BW_DL:= 0.05 * b_{AS};
	ENDIF;
	ELSE
	Max_BW_UL:= as set by the UE manufacture;
	Max_BW_DL:= as set by the UE manufacture;
	ENDIF;
	ENDIF;
	ENDIF;

Maximum Authorized QoS Class Identifier [QCI] per flow identifier (see NOTE 1, 2 and 3)	IF (all media IP flows of media type "audio" or "video" for the session are unidirectional and have the same direction) THEN
	MaxService:= 3 or 4;
	ELSE
	MaxService:= 1 or 2;
	ENDIF;
	
	CASE <media> OF
	"audio": QCI:= MaxService;
	"video": QCI:= MaxService;
	"application": QCI:=1 or 2;
	"data": QCI:=6 or 7 or 8;
	"control": QCI:=5;
	/*new media type*/
	OTHERWISE: QCI:=9;
	END;

NOTE 1: The Maximum Authorized QoS Class Identifier for a RTCP IP flow is the same as for the corresponding RTP media IP flow.
NOTE 2: When audio or video IP flow(s) are removed from a session, the parameter MaxService shall keep the originally assigned value.
NOTE 3: When audio or video IP flow(s) are added to a session, the UE shall derive the parameter MaxService taking into account the already existing media IP flows within the session
NOTE 4: The SDP parameters are described in RFC 2327 [15].
NOTE 5: The 'b=RS:' and 'b=RR:' SDP bandwidth modifiers are defined in RFC 3556 [16].

6. Interworking between EPC and external PDNs

6.1 Functional Entities

6.1.1 PDN GW

The PDN GW is the gateway which terminates the SGi interface towards the PDN. If a UE is accessing multiple PDNs, there may be more than one PDN GW for that UE. From the external IP network's point of view, the PDN GW is seen as a normal IP router.

6.2 Procedures

6.3 Protocol impacts

6.3.1 Protocol impacts on SGi

SGi is the reference point between the PDN Gateway and the packet data network. Packet data network may be an operator external public or private packet data network or an intra operator packet data network, e.g. for provision of

IMS services. This reference point corresponds to Gi and Wi functionalities and supports any 3GPP and non-3GPP access systems.

7. QoS mechanisms

7.1 Functional Entities

7.1.1 PCRF

PCRF makes the QoS authorization for an SDF and provides it to the PCEF over the Gx interface. The authorized QoS for the SDF consists of a QoS Class Identifier (QCI), Allocation and Retention Priority (ARP) and authorized Guaranteed and Maximum Bit Rate values for uplink and downlink.

The QCI is access agnostic, i.e. standardized QCIs and corresponding characteristics are independent of the UE's current access. It is not required that an IP-CAN supports all standardized QCIs. The PCRF selects a QCI based on IP-CAN information. The PCRF identifies the IP-CAN by the IP-CAN Type and RAT Type AVPs which the PCRF gets from the PCEF upon the initial attach to the radio network or upon a possible later access network type change.. If a set of service information which can not be served by the current IP-CAN system is received from the AF, the PCRF should reject it.

Editor's note: It is FFS at stage 2 (refer to TS 23.401 / 4.7.4) whether the PCRF may select a different QCI due to a handover to a different RAT type.

For E-UTRAN and for the same UE/PDN connection, SDFs associated with different QCIs shall not be mapped to the same EPS bearer.

7.1.2 PCEF

The bearer level QCI of an EPS bearer is identical to the value of the QCI of the SDF(s) mapped to that EPS bearer In this way, a mapping from the service level QCI to the bearer level QCI is not required in the PCEF.

The PCEF maps the QCI to transport network level QoS parameter values according to the prevailing/used access network type.

Editor's note: A mapping between standardized QCIs and transport network level QoS parameter values is still open in stage 2 (refer to TS 23.401 / Annex B).

7.2 Procedures

7.2.1 Transport network level packet marking

Transport Network Level (TNL) packet marking is carried out by the P-GW and S-GW as defined in 3GPP TS 23.401 [2]. The P-GW and S-GW may carry out TNL marking in the downlink and uplink directions. In the P-GW uplink and downlink TNL marking is used on the S5/S8 interfaces. In the S-GW uplink TNL marking is used on the S5/S8 interfaces and downlink TNL marking on the S2 interface when a non-3GPP access is anchored on the S-GW. Both P-GW and S-GW may use transport network level packet marking in order to set the DSCP codes of the TNL packets based on the QCI of the associated EPS bearer.

NOTE 1: For GTP-based networks the QCI is known implicitly by the S-GW since it is part of the EPS QoS profile associated with a GTP TEID

NOTE 2: For PMIP-based networks the QCI is known explicitly through the provisioning of policy rules to the policy enforcement functions within the P-GW/S-GW

7.3 Protocol impacts

7.3.1 Protocol impacts on Gx

The authorized QoS for the SDF is conveyed in a PCC rule over the Gx interface. It comprises a QCI and the relevant GBR and MBR for both uplink and downlink. The QCI is a scalar that represents the QoS characteristics that the EPS is expected to provide for the SDF.

The bearer level QCI of an EPS bearer is identical to the value of the QCI of the SDF(s) mapped to that EPS bearer.

The QCI is access agnostic, i.e. standardized QCIs and corresponding characteristics are independent of the UE's current access. It is not required that an IP-CAN supports all standardized QCIs. The PCRF selects a QCI based on IP-CAN information. The PCRF identifies the IP-CAN by the IP-CAN Type and RAT Type AVPs which the PCRF gets from the PCEF upon the initial attach to the radio network or upon a possible later access network type change.

Editor's note: It is FFS at stage 2 (refer to TS 23.401 / 4.7.4) whether the PCRF may select a different QCI due to a handover to a different RAT type.

Editor's note: SA2 has defined QCI characteristics in stage 2 TS 23.401 / Annex C (Informative). However, the work is still in progress. The intention is to move the definition of the QCI characteristics to the stage 2 TS 23.203.

Editor's note: A new RAT Type value is required for E-UTRAN. (RAT Type values are defined in TS 29.060).

8. E-MBMS

Editor's Note: It is FFS if the CP and UP functions of the MBMS entity are separated and connected with a reference point in between or if it is one entity handling both MBMS CP and UP functions.

8.1 Functional Entities

8.1.1 MBMS CP

8.1.2 MBMS UP

8.1.3 eBM-SC

8.1.4 PDN-GW

NOTE: No special work for this function entity in CT3 is expected.

8.2 Protocols

8.2.1 Protocol for SGi-mb interface

8.2.2 Protocol for SGmb interface

8.2.3 Protocol for SGi interface

NOTE: No special work for this interface in CT3 is expected.

9. SAE impact on existing capabilities

9.1 GPRS MBMS

9.2 Lawful Interception

9.3 Trace

10. Conclusion

Annex A : Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
08/02/2007					Skeleton	-	0.0.0
15/02/2007					First official version	0.0.0	0.1.0
18/08/2007					CRs implemented: C3-070838, C3-070888, C3-070884, C3-070682, C3-070841	0.1.1	0.2.0
16/11/2007					CRs implemented: C3-071106, C3-071107, C3-071143, C3-071144, C3-071145, C3-071146, C3-071164.	0.2.0	0.3.0
08/02/2008					CRs implemented: C3-080030, C3-080161, C3-080193, C3-080195, C3-080196, C3-080205, C3-080206, C3-080220, C3-080221, C3-080224, C3-080230, C3-080231, C3-080250.	0.3.0	0.4.0
18/02/2008					Implementation of C3-080195 fixed.	0.4.0	0.4.1
08/04/2008					CRs implemented: C3-080406, C3-080408, C3-08414, C3-080423, C3-080426, C3-080440, C3-080441, C3-080442, C3-080443, C3-080444, C3-080445, C3-080447, C3-080448, C3-080449, C3-080450, C3-080451, C3-080453	0.4.1	0.5.0
19/05/2008					CRs implemented: C3-080734, C3-080737, C3-080742, C3-080743, C3-080746, C3-080780, C3-080804, C3-080805, C3-080806, C3-080820, C3-080830, C3-080834, C3-080835	0.5.0	0.6.0
20/05/2008					Editorial correction	0.6.0	0.6.1
21/05/2008					Version 1.0.0 created for presentation to TSG	0.6.1	1.0.0
30/06/2008					CRs implemented: C3-081240, C3-081244 Also implemented C3-080853, as result of email approval process from last meeting CT3#48 (already included in v070 but missing in v100) Editor's notes formatting	1.0.0	1.1.0
26/08/2008					CRs implemented: C3-081536, C3-081687	1.1.0	1.2.0
01/09/2008					Version 2.0.0 created for presentation to TSG by MCC	1.2.0	2.0.0
16/09/2008	TSG #41				Version 8.0.0 created by MCC	2.0.0	8.0.0
17/12/2008	TSG #42				Upgraded to v8.0.1 due to simple upgrade without no technical change	8.0.0	8.0.1