Policy and Charging Rules Function (PCRF) in LTE EPC Core Technology

Prepared by
Mojtaba HOUSHMAND

2016 - August

Table of Contents

(1) LTE EPC Technology Essentials

LTE (both radio and core network evolution) is now on the market. Release 8 was frozen in December 2008 and this has been the basis for the first wave of LTE equipment. LTE specifications are very stable, with the added benefit of enhancements having been introduced in all subsequent 3GPP Releases.

The motivation for LTE

- Need to ensure the continuity of competitiveness of the 3G system for the future
- User demand for higher data rates and quality of service
- Packet Switch optimized system
- Continued demand for cost reduction (CAPEX and OPEX)
- Low complexity
- Avoid unnecessary fragmentation of technologies for paired and unpaired band operation

1.1 LTE Overview

LTE (Long Term Evolution) or the E-UTRAN (Evolved Universal Terrestrial Access Network), introduced in 3GPP R8, is the access part of the Evolved Packet System (EPS). The main requirements for the new access network are high spectral efficiency, high peak data rates, short round trip time as well as flexibility in frequency and bandwidth.

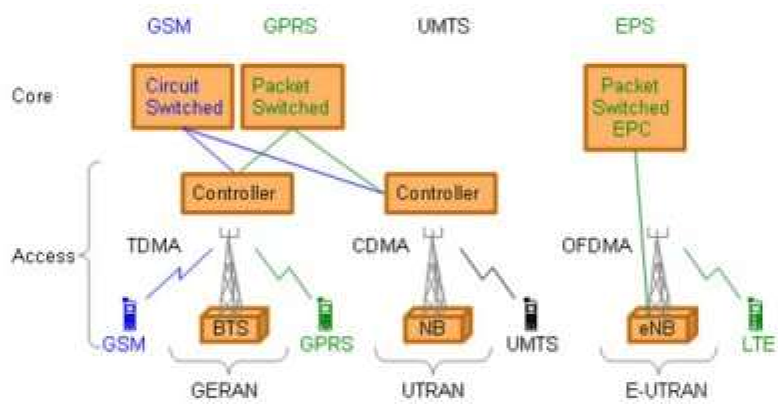


Figure 1.1: Network Solutions from GSM to LTE

GSM was developed to carry real time services, in a circuit switched manner (blue in figure 1), with data services only possible over a circuit switched modem connection, with very low data rates. The first step towards an IP based packet switched (green in figure 1) solution was taken with the evolution of GSM to GPRS, using the same air interface and access method, TDMA (Time Division Multiple Access).

To reach higher data rates in UMTS (Universal Mobile Terrestrial System) a new access technology WCDMA (Wideband Code Division Multiple Access) was developed. The access network in UMTS emulates a circuit switched connection for real time services and a packet switched connection for datacom services (black in figure 1). In UMTS the IP address is allocated to the UE when a datacom service is established and released when the service is released. Incoming datacom services are therefore still relying upon the circuit switched core for paging.

1.2 EPC Core Overview

The EPC is the latest evolution of the 3GPP core network architecture.

In GSM, the architecture relies on circuit-switching (CS). This means that circuits are established between the calling and called parties throughout the telecommunication network (radio, core network of the mobile operator, fixed network). This circuit-switching mode can be seen as an evolution of the "two cans and a string". In GSM, all services are transported over circuit-switches telephony principally, but short messages (SMS) and some data is also seen.

In GPRS, packet-switching (PS) is added to the circuit-switching. With this technology, data is transported in packets without the establishment of dedicated circuits. This offers more flexibility and efficiency. In GPRS, the circuits still transport voice and SMS (in most cases). Therefore, the core network is composed of two domains: circuit and packet.
In UMTS (3G), this dual-domain concept is kept on the core network side. Some network elements have evolved but the concept remains very similar.

When designing the evolution of the 3G system, the 3GPP community decided to use IP (Internet Protocol) as the key protocol to transport all services. It was therefore agreed that the EPC would not have a circuit-switched domain anymore and that the EPC should be an evolution of the packet-switched architecture used in GPRS/UMTS.
This decision had consequences on the architecture itself but also on the way that the services were provided. Traditional use of circuits to carry voice and short messages needed to be replaced by IP-based solutions in the long term.

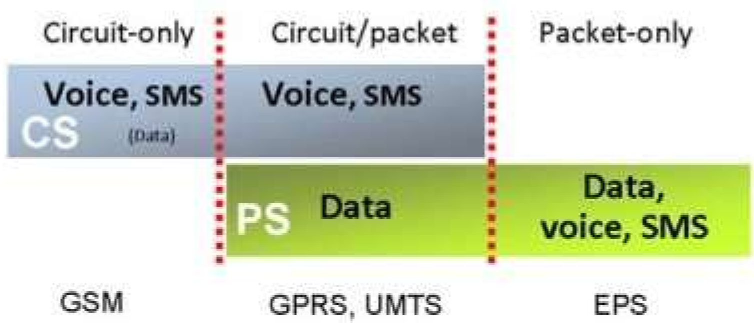
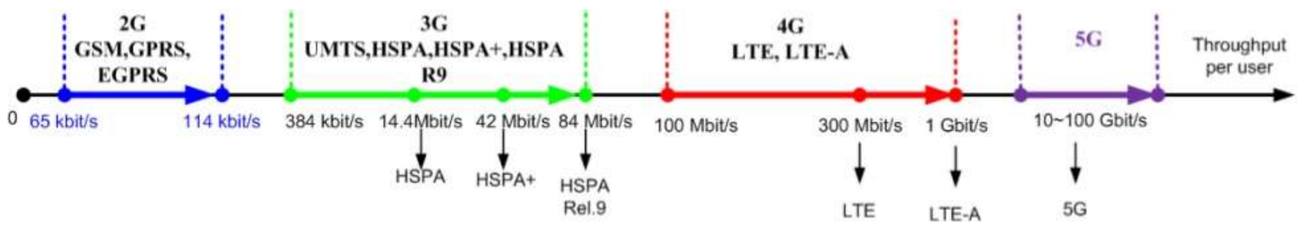


Figure 1.2: Circuit and Packet Domains

(2) 2G/3G vs LTE Roadmap

Adopt the user requirements for high speed data and efficient quality:



2G GPRS Mobile Technology was the first step to provide data services over the mobile networks.

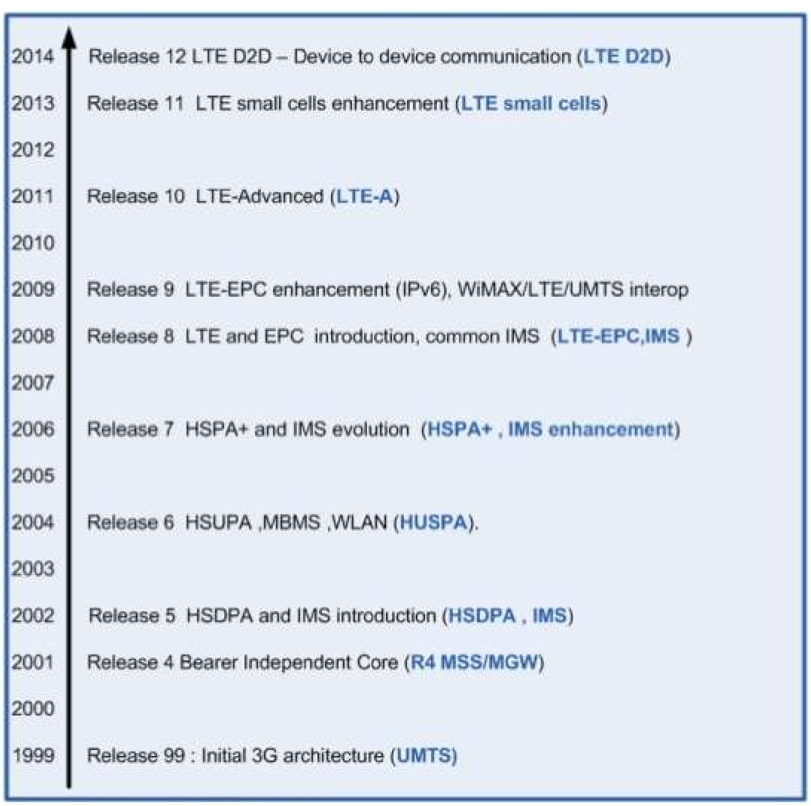
3G Technology provides a higher data rates support with better integrity.

LTE has the biggest challenge to overcome over the later technologies.

LTE is compatible with the current 2G/3G Network as it is counted as the next step of 3G HSPA Network.
LTE have been developed by the same standard group of 2G/3G (3gpp).

Release 13, IOT and M2M integration and Customization of RAN plus major enhancement for LTE feature (SRVCC, power reduction).

Release 14, Introduction of 5G Networks "Next Generation".



Following table compares various important Network Elements & Signaling protocols used in 2G/3G and LTE.

2G/3G	LTE
GERAN and UTRAN	E-UTRAN
SGSN/PDSN-FA	S-GW
GGSN/PDSN-HA	PDN-GW
HLR/AAA	HSS
VLR	MME
SS7-MAP/ANSI-41/RADIUS	Diameter
DiameterGTPc-v0 and v1	GTPc-v2
MIP	PMIP

(3) Evolved Packet Core (EPC) and its Component

The EPC (Evolved Packet Core) is composed of several functional entities:

- The MME (Mobility Management Entity)
- The HSS (Home Subscriber Server)
- The Serving Gateway.
- The PDN Gateway (Packet Data Network).
- The PCRF (Policy and Charging Rules Function) Server.

The following sub-sections discuss each of these in detail:

3.1 MME (Mobility Management Entity)

The MME is in charge of all the Control plane functions related to subscriber and session management. From that perspective, the MME supports the following:

- Security procedures – this relates to end-user authentication as well as initiation and negotiation of ciphering and integrity protection algorithms.
- Terminal-to-network session handling – this relates to all the signaling procedures used to set up Packet Data context and negotiate associated parameters like the Quality of Service.
- Idle terminal location management – this relates to the tracking area update process used in order for the network to be able to join terminals in case of incoming sessions.

The MME is linked through the S6 interface to the HSS which supports the database containing all the user subscription information.

3.2 HSS (Home Subscriber Server)

The HSS (Home Subscriber Server) is the concatenation of the HLR (Home Location Register) and the AuC (Authentication Center) – two functions being already present in pre-IMS 2G/GSM and 3G/UMTS networks. The HLR part of the HSS is in charge of storing and updating when necessary the database containing all the user subscription information, including (list is non exhaustive):

- User identification and addressing – this corresponds to the IMSI (International Mobile Subscriber Identity) and MSISDN (Mobile Subscriber ISDN Number) or mobile telephone number.
- User profile information – this includes service subscription states and user-subscribed Quality of Service information (such as maximum allowed bit rate or allowed traffic class).

The AuC part of the HSS is in charge of generating security information from user identity keys. This security information is provided to the HLR and further communicated to other entities in the network. Security information is mainly used for:

- Mutual network-terminal authentication.
- Radio path ciphering and integrity protection, to ensure data and signaling transmitted between the network and the terminal is neither eavesdropped nor altered.

3.3 The Serving GW (Serving Gateway)

From a functional perspective, the Serving GW is the termination point of the packet data interface towards E-UTRAN. When terminals move across eNodeB in E-UTRAN, the Serving GW serves as a local mobility anchor, meaning that packets are routed through this point for intra E-UTRAN mobility and mobility with other 3GPP technologies, such as 2G/GSM and 3G/UMTS.

3.4 The PDN GW (Packet Data Network Gateway)

Similarly, to the Serving GW, the PDN gateway is the termination point of the packet data interface towards the Packet Data Network. As an anchor point for sessions towards the external Packet Data Networks, the PDN GW also supports Policy Enforcement features (which apply operator-defined rules for resource allocation and usage) as well as packet filtering (like deep packet inspection for virus signature detection) and evolved charging support (like per URL charging).

3.5 The PCRF (Policy and Charging Rules Function) Server

The PCRF server manages the service policy and sends QoS setting information for each user session and accounting rule information. The PCRF Server combines functionalities for the following two UMTS nodes:

- The Policy Decision Function (PDF)
- The Charging Rules Function (CRF)

The PDF is the network entity where the policy decisions are made. As the IMS session is being set up, SIP signaling containing media requirements are exchanged between the terminal and the P-CSCF. At some time in the session establishment process, the PDF receives those requirements from the P-CSCF and makes decisions based on network operator rules, such as:

- Allowing or rejecting the media request.
- Using new or existing PDP context for an incoming media request.
- Checking the allocation of new resources against the maximum authorized

The CRFs role is to provide operator-defined charging rules applicable to each service data flow. The CRF selects the relevant charging rules based on information provided by the P-CSCF, such as Application Identifier, Type of Stream (audio, video, etc.), Application Data Rate, etc.

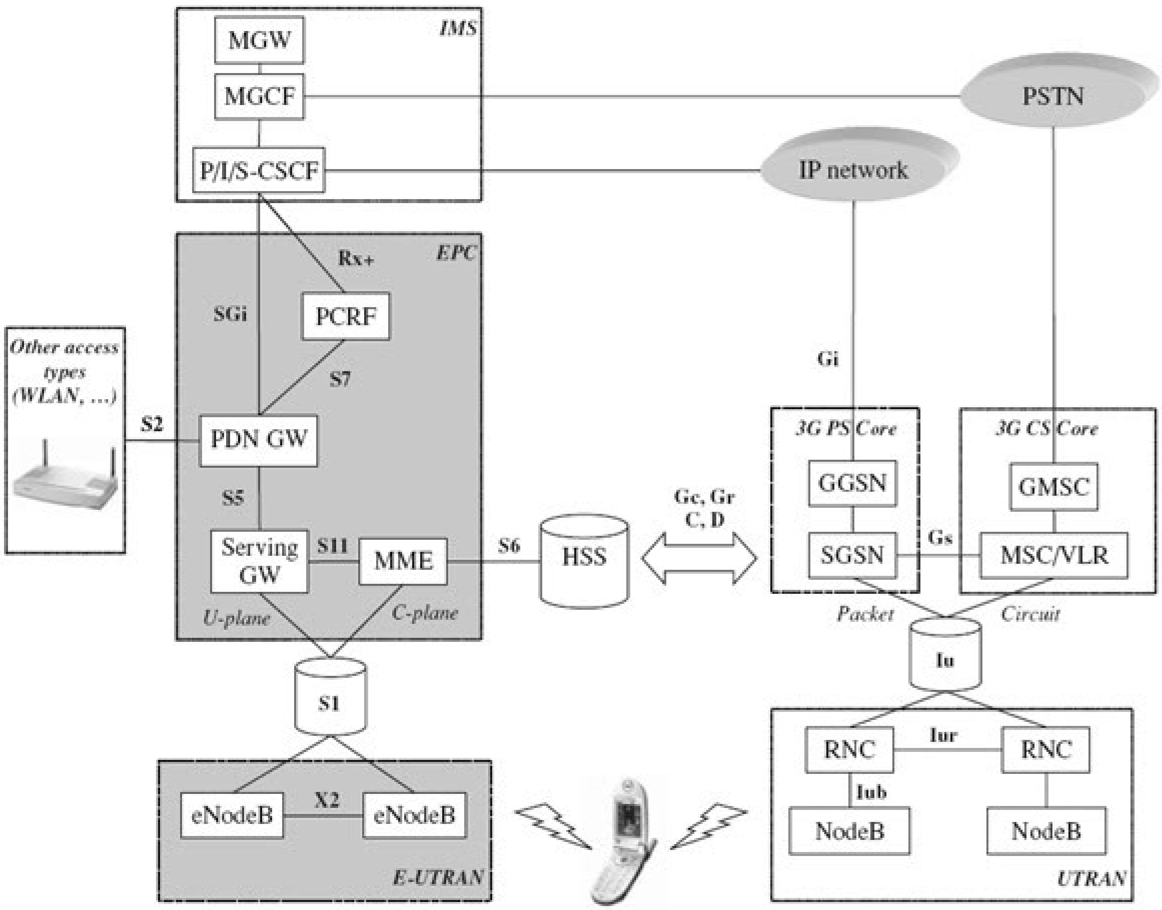


Figure 3: Evolved Packet Core (EPC) and its Component

(4) Introduction of PCRF

The convergence of broadband access, virtually unlimited content and smart mobile devices has permanently altered the telecommunications market. Demand for mobile Internet services is rapidly increasing day by day as customers want to receive their content, media and applications on any device at any time. For the last few years, the telecom industry is radically transforming the revenue streams, business models and value chains.

To remain relevant in this rapidly changing environment, telecom operators must address critical challenges to create new business models and reinvent themselves.

Therefore, Service Provider must have some statistics that determine how and under what conditions subscribers and applications use network resources for formulation of the policies. The Policy Server manages policy rules between applications and policy enforcement points like access devices. It can easily add and re-configure policies to dynamically manage and control Quality of Service (QoS),

charging, quota, optimization and admission control. A wide variety of interfaces make it easy to integrate the PCRF with any type of mobile or fixed broadband network.
Since operators will be migrating from 2G to 3G to 4G networks in years to come, existing networks must operate concurrently with newer networks. As subscribers travel between mobile networks, and also the fixed network, operators must be able to maintain session visibility. As a result, policy solutions must be able to dynamically control sessions per subscriber.
PCRF can provide a network agnostic solution (wire line and wireless) and can also enable multi-dimensional approach which helps in creating a lucrative and innovative platform for operators. PCRF can also be integrated with different platforms like billing, rating, charging, and subscriber database or can also be deployed as a standalone entity.

(5) Definition of PCRF & Need

Policy and Charging Rules Function (PCRF) is a node which functions in real-time to determine policy rules in a multimedia network. As a policy tool, the PCRF plays a central role in next-generation networks/LTE. It is a component that operates at the network core and accesses subscriber databases and other specialized functions, such as a charging system, in a centralized manner. The PCRF has an increased strategic significance and broader potential role, than traditional policy engines, due to its working in real time.
The PCRF is the part of the network architecture that aggregates information to and from the network, operational support system and other sources (such as portals) in real time, supporting the creation of rules and then automatically making policy decisions for each subscriber active on the network. Such a network might offer multiple services, quality of services (QoS) levels, and charging rules.

It provides:

- The ability to manage network and subscriber policy in real time.
- The ability to efficiently and dynamically route and prioritize network traffic.
- Unified view of subscriber context based on a combination of device, network, location and billing data.
- Key inputs to revenue assurance and bandwidth management.

Policy and Charging Rules Function (PCRF) is the part of the Evolved Packet Core (EPC) that supports service data flow detection, policy enforcement and flow-based charging.

PCRF plays a key role in VoLTE as a mediator of network resources for the IP Multimedia Systems network for establishing the calls and allocating the requested bandwidth to the call bearer with configured attributes. This enables an operator to offer differentiated voice services to their user(s) by charging a premium. Operators also have an opportunity to use PCRF for prioritizing the calls to emergency numbers in the next-gen networks.

Dedicated policy equipment standardized in 3GPP that enables the policy function for bandwidth and charging on multimedia networks.
PCRF is a fairly new term, introduced in September 2007 when standards for the 3GPP Policy Charging Control (PCC) architecture were published. The PCRF function is part of the larger PCC architecture, which also includes the Proxy Call Session Control Function (P-CSCF) and the Policy and

Charging Enforcement Function (PCEF). Combined, the elements of the PCC provide access, resource, and quality-of-service (QoS) control.
PCRF is often referred to as policy server or -- formerly -- a Policy Decision Function (PDF).
PCRF is an important element in Service Provider Information Technology (SPIT). The PCRF interfaces with the main packet gateway and takes charging enforcement decisions on its behalf. The centralized device can act as a policy decision point (PDP) for the wireless operator and gets as granular as individual subscribers.

For example, service providers can use PCRF to charge subscribers based on their volume of usage of high-bandwidth applications, charge extra for QoS guarantees, limit app usage while a user is roaming, or lower the bandwidth of wireless subscribers using heavy-bandwidth apps during peak usage times.

5.1 The Policy and Charging Challenge

Policy and Charging rules are driven by the PCRF (Policy Charging and Rules Function), PCEF (Policy Control Enforcement Function) and the Charging Functions in the IMS and EPC core networks. These elements provide carriers with the ability to differentiate services while maximizing revenue.
Every carrier service has unique bandwidth requirements. Policy control within the PCRF and PCEF ensures that appropriate amounts of bandwidth are dynamically allocated to each service in real time, thus making the most efficient use of network resources. Prior to launching a new service like VoLTE, carriers need to test and validate their policy rules within the PCRF and PCEF to ensure the services are delivered with integrity and to ensure that there is sufficient capacity to provide the requested services. Charging rules are very similar and also must be validated. A service provider may implement a multitude of charging rules for each service; and these rules may differ based on a variety of conditions, for example: Customer Service Level Agreement, time of day, or network conditions.

5.2 Need for PCRF - Following two cases describe the need of PCRF in telecom network:

5.2.1 Changing Revenue Streams

In many developed telecom markets, voice revenue has gained a peak and has declining trends. Messaging is expected to increase globally significantly in coming years. New IP message services like iMessage and WhatsApp are beginning to attract consumers' attention, particularly those with smart phones. As the IP messaging phenomena takes off, SMS messaging revenues will also decline.
Data access is still a growth engine for operators and is helping in compensating the decline in voice and messaging revenues. In major markets, data demand is doubling each year, but margin pressure is intense. At present, expenditure incurred in building network capacity to handle the increasing load is more than the revenue earned by data access.
In view of above, operators need to plan new revenue streams. For implementation of this operators need a PCRF type entity in their telecom network.

5.2.2 Business Transformation Starts with the Network

Existing telecom networks are not built with the DNA (Dynamic Network Administration) to foster innovation and respond quickly to dynamic markets to meet the demands of the subscribers. To reinvent themselves, operators need to redesign their legacy infrastructure into a highly evolved,

completely software-defined network (SDN) –the thinking network. The thinking network is analogous to the human body.
The memory is the subscriber database. The language is the Diameter protocol, the central nervous system is the new product category of Diameter Signaling Controller (DSC), and the brain is policy.

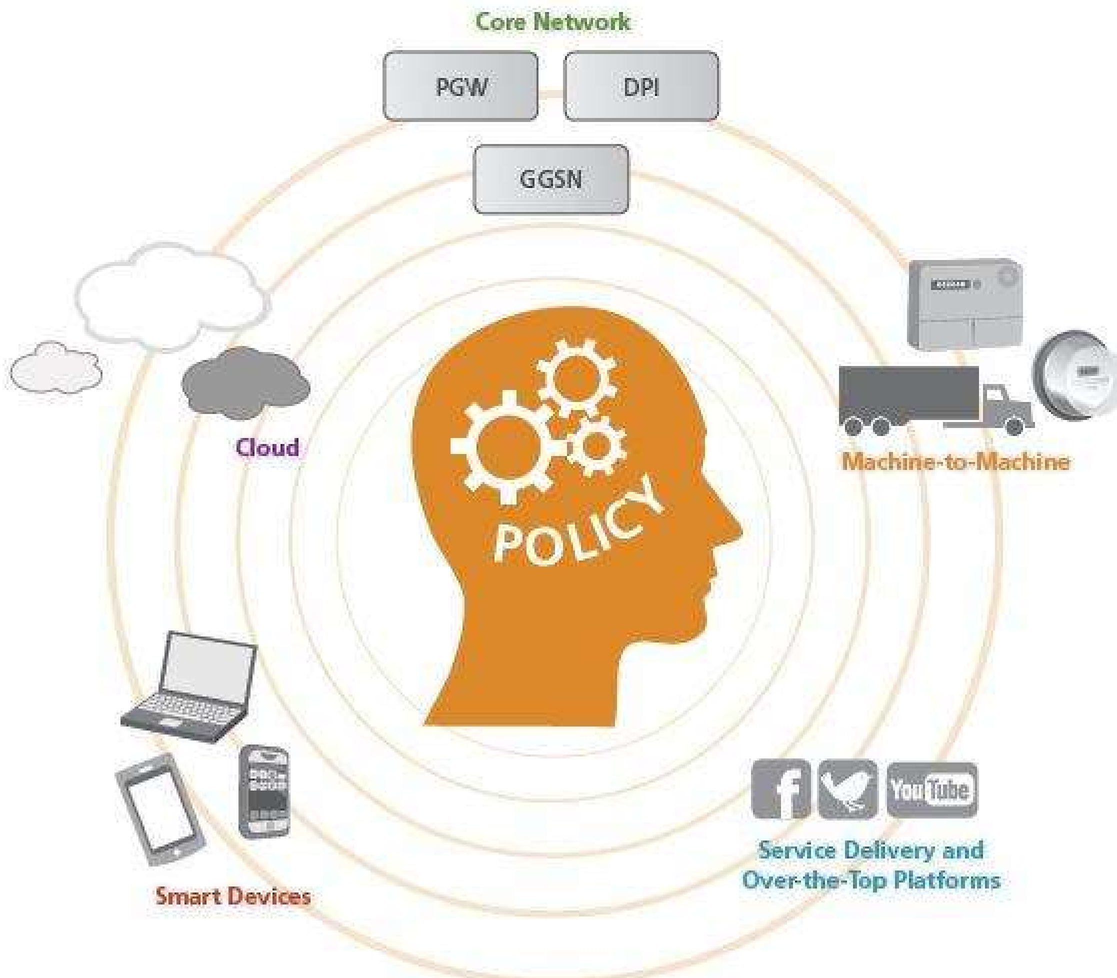


Figure 5.2.2: Thinking Network

(6) How does policy control and charging works in LTE?

An important component in LTE network is the policy and charging control (PCC) function that brings together and enhances capabilities from earlier 3GPP releases to deliver dynamic control of policy and charging on a per subscriber and per IP flow basis.
LTE Evolved Packet Core (EPC) EPC includes a PCC architecture that provides support for fine-grained QoS and enables application servers to dynamically control the QoS and charging requirements of the services they deliver. It also provides improved support for roaming. Dynamic control over QoS and charging will help operators monetize their LTE investment by providing customers with a variety of QoS and charging options when choosing a service.

The LTE PCC functions include:

- PCRF (policy and charging rules function) provides policy control and flow based charging control decisions.
- PCEF (policy and charging enforcement function) implemented in the serving gateway, this enforces gating and QoS for individual IP flows on the behalf of
- the PCRF. It also provides usage measurement to support charging
- OCS (online charging system) provides credit management and grants credit to the PCEF based on time, traffic volume or chargeable events.
- OFCS (off-line charging system) receives events from the PCEF and generates charging data records (CDRs) for the billing system.

(7) PCRF - The Architecture

PCRF was introduced in September 2007 when standards for the 3GPP Policy Charging Control (PCC) architecture were published. The PCRF function is part of the larger PCC architecture, which also includes the Proxy Call Session Control Function (P-CSCF) and the Policy and Charging Enforcement Function (PCEF). Combined, the elements of the PCC provide access, resource, and quality-of-service (QoS) control.

PCRF is an important part of IMS architectures, although it is not exclusive to the 3GPP-based network in which it was certified. It works across wireless networks and can be deployed on carrier grade/ATCA (Advanced Telecommunications Computing Architecture)/COTS (Commercial off the shelf) hardware.

The PCRF interfaces with the main packet gateway and takes charging enforcement decisions. The centralized device can act as a policy decision point (PDP) for the wireless operator and goes down to the individual subscribers.

Service providers can use PCRF to facilitate for charging of subscribers based on their volume of usage of high-bandwidth applications and charging based on QoS guarantees, limit app usage while a user is roaming, or lower the bandwidth of wireless subscribers using heavy-bandwidth apps during peak usage times.

PCRF Server is carrier grade platform used to implement the convergent policy management, real-time policy decision solutions across core network domain and content application domain for the network service providers.

PCRF Server includes a 3GPP-compliant implementation of Policy and Charging Rules Function to provision, manage and execute the Quality of Service policies, Bandwidth control policies, Subscriber-aware policies, and Application gating policies in the 2G/3G and LTE networks.

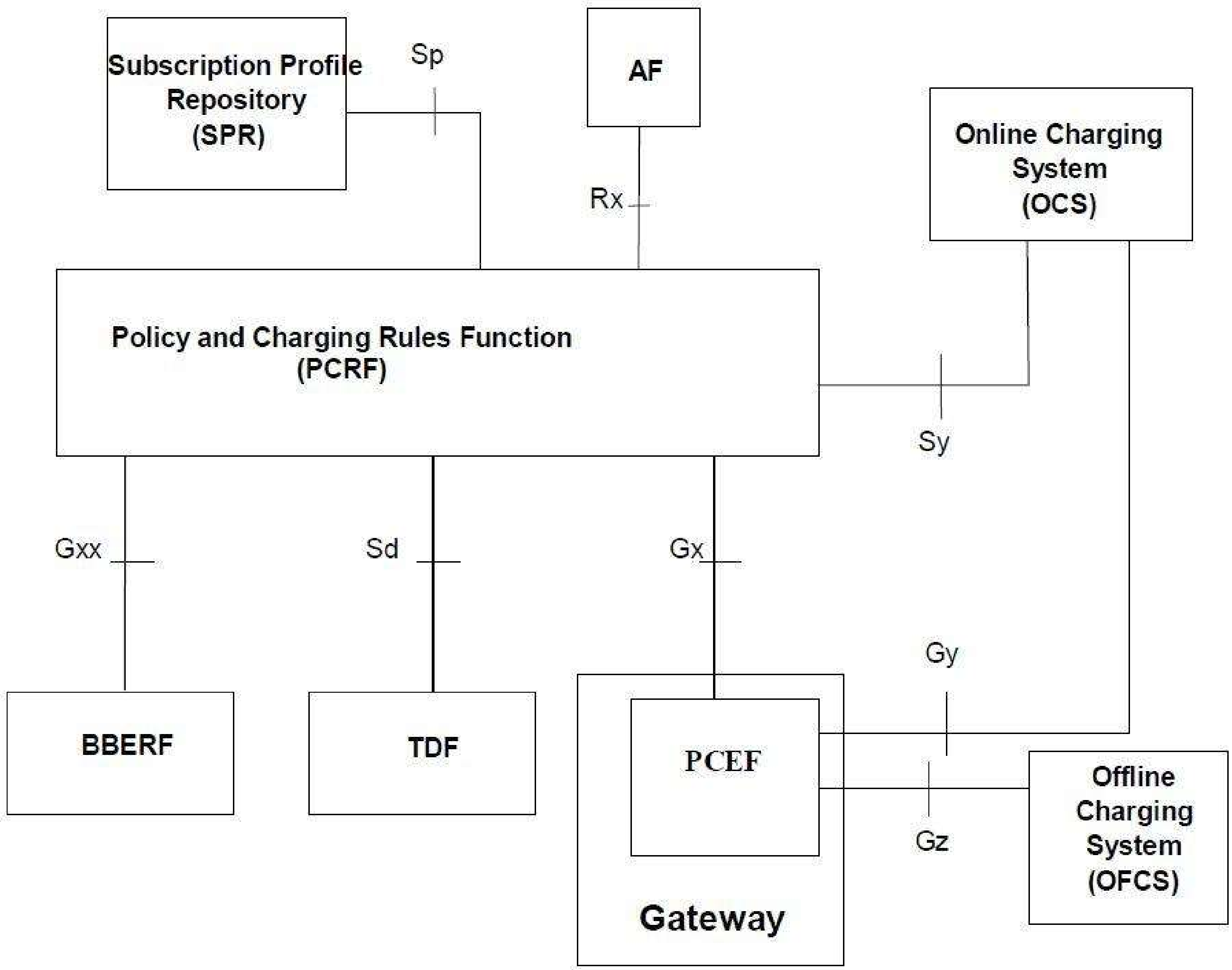


Figure 7: as per 3GPP TS 23.203

Legends:
PCEF: Policy and Charging Enforcement function
TDF: Traffic Detection Function
AF: Application Function
BBERF: Bearer Binding and Event Reporting Function

PCRF is comprised of the following components/subsystems
a. One or more policy servers which provides the policy and charging management functions
b. Subscriber Profile Repositories (SPR)
c. A Configuration Central Management Subsystems for centralized provisioning and management of the policy servers

7.1 Policy Server

The PCRF SERVER is the main server engine that processes the policy requests from the core network elements or B/OSS (Business/Operations Support System) systems at real-time. The main components of the PCRF Server are the Diameter-based 3GPP Gx, Rx, Sy, Gxx, Sp and Sd Connectors, Policy and Charging Rules Server, Policy Decision Platform, Subscriber Profile Cache and Subscription Management Service.

The Policy Server has a rules engine and acts as the standards based Policy Charging and Rules Function (PCRF) in the network. The rules engine operates on triggers, processes conditions, and then performs appropriate action(s) based on the conditions. The rules engine can be invoked based on any interface trigger. The rules engine can be triggered by a message from either the GGSN or DPI via either the Gx interface, the SPR via the Sp or SOAP/XML interface, as well as the application function via the Rx interface. The rules engine can also be triggered by internal timers which can be used to support a variety of time of day based applications/use cases. Policies can be developed quickly using Policy Rules wizard.

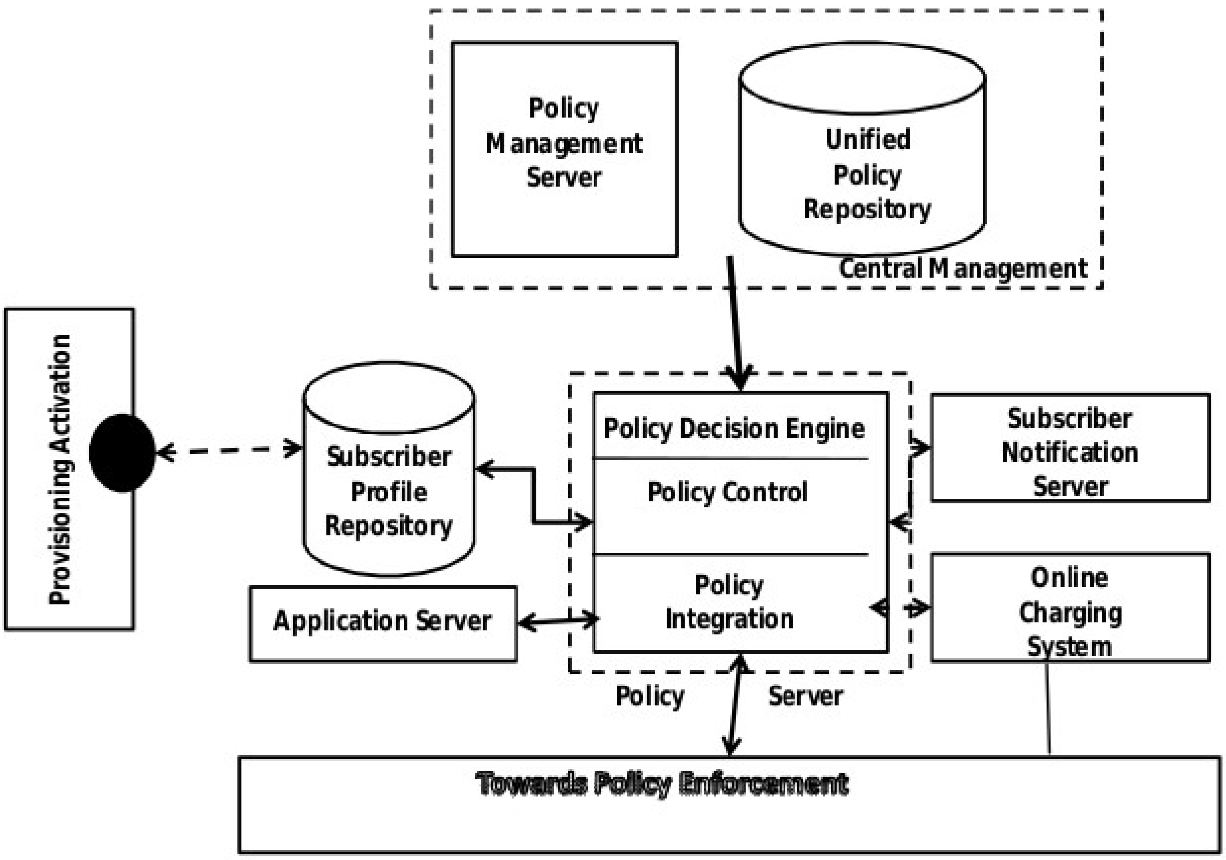


Figure 7.1: PCRF's Subsystems

7.2 SPR- Subscriber Profile Repository

SPR is the repository to store all business assets, technical assets and configuration items used by the PCRF Server, Central Management Server. This is a mandatory component to run PCRF Server.
Policy's SPR should act as the policy solution database to store subscriber profile, quota, and state information of the Policy Server to use in its policy execution. The SPR should be deployed in networks to store subscriber profile information and inter-session state information (e.g. usage and quota tracking). The SPR should be deployed in a variety of configurations according to the customer needs and requirements e.g. in a standalone redundant HW configuration or together with the other PCRF components within the same platform.

7.3 Policy Management Platform/Central Management Subsystem

Central Management Subsystem is the centralized server node to monitor and manage the PCRF Server and Repository Server. It's the core component for PCRF Server to provide the OA&M functions. The Management Platform provides a consolidated view of system alarms and logs and has SOAP/ XML API to interface to external systems.
In addition to above, PCRF server may also have following Components/functionalities:

(a) SPR Proxy subsystem - It is a component that exposes the Web Services API within PCRF Server for management of the internal Subscriber Profile Repository (that is, subscriptions and subscribers).

(b) Load Balancer – It is the key component in the distributed deployment environment for PCRF Server. It provides the Diameter application level load balancing capability.

(8) Deployment of PCRF in Telecom Network

Following are the architecture of telecom network with PCRF.

8.1 PCRF with 2G/3G Network

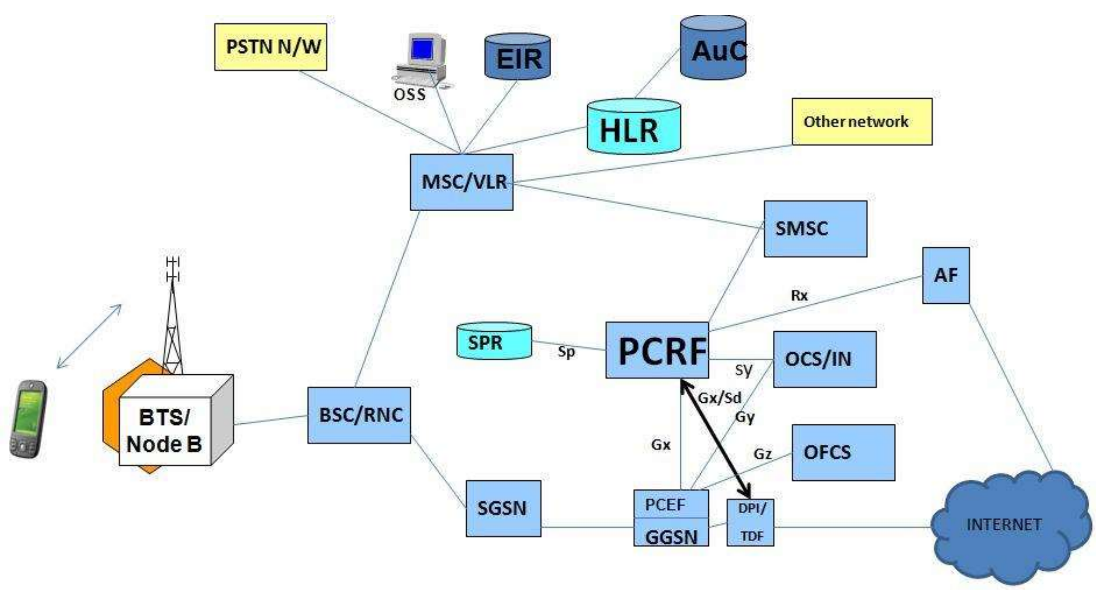


Figure 8.1: PCRF with 2G/3G Network

8.2 PCRF with 4G/LTE Network

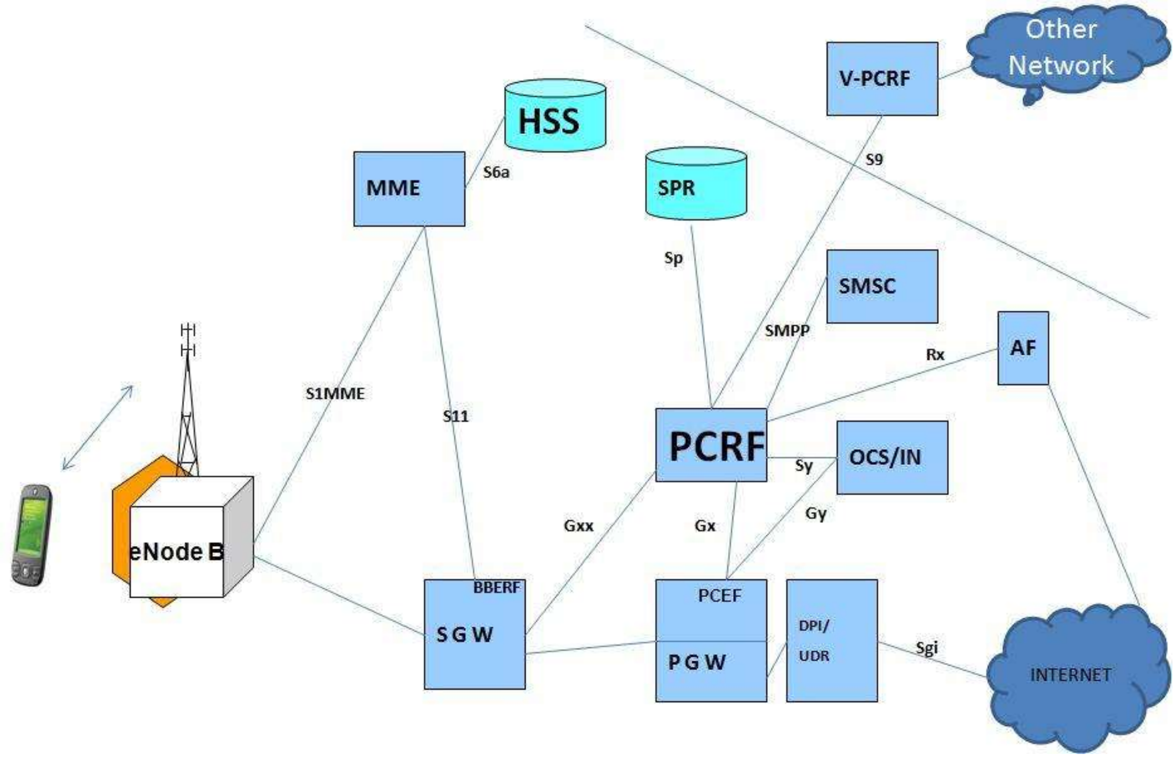


Figure 8.2: PCRF with 4G/LTE Network

8.3 PCRF in converged network

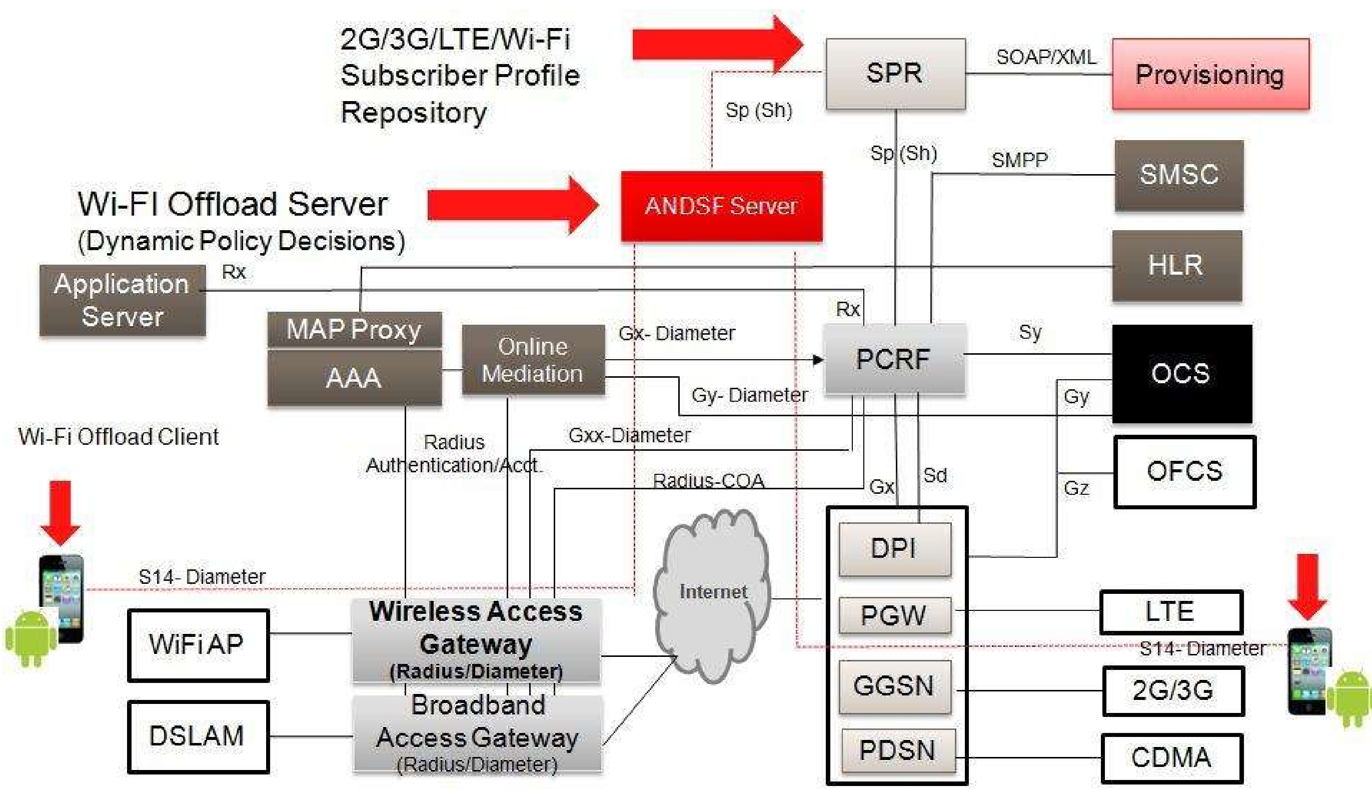


Figure 8.3: PCRF in converged network

8.4 PCRF Supported Interfaces

Following are the description of used external interfaces supported by PCRF Server:

(i) Gx Interface - PCRF Server supports the Gx interface as defined in 3GPP Release 7, 8, 9 and 10. It is used for provisioning service data flow based on charging rules. It is located between the PCRF and the Policy and Charging Enforcement Function (PCEF). In most cases, PCEF is based inside PDN GW (Packet Data Network Gateway) or in short PGW, as in above diagram.
PCRF Server is very flexible and can be configured to support any specific AVPs in the network element and accommodate customer specific scenarios.

(ii) Gy Interface - PCRF Server supports the Gy interface and acts as DCCA proxy between PCEF and OCS (Online Charging System). This interface allows online credit control for service data flow based charging.

(iii) Gz Interface – This is used for offline (CDR based) charging interface between the PCEF/PDN GW and OFCS (Offline Charging system).

(iv) Rx Interface - PCRF Server supports the Rx interface as defined in 3GPP Release 10. This reference points are used to exchange application level session information & media related information between the PCRF & Application function/Application Server. This information is the part of the inputs used by the PCRF for the Policy and Charging Control Decisions.
(v) Sy Interface - PCRF Server supports the Sy interface as defined in 3GPP Release 11. It is used between PCRF and OCS for sending limits reports.

(vi) Sp Interface - PCRF Server supports the Sp interface between the PCRF and the SPR. This interface allows the PCRF to request subscription information related to transport level policies from the SPR based on a subscriber ID, a PDN identifier and possible further IP CAN session attributes, as specified in 3GPP TS 23.203 v9.x. This interface allows the SPR to notify the PCRF when the subscription information has been changed if the PCRF has requested such notifications. The SPR shall stop sending the updated subscription information when a cancellation notification request has been received from the PCRF.

(vii) Ud Interface - PCRF Server supports the Ud interface between the PCRF and the UDR. This interface allows the PCRF to create, read, modify and delete user data stored in the UDR using the access interface. It is based in LDAP. This interface supports subscriptions/notifications functionality to allow the PCRF being notified about specific events that may occur on specified user data in the UDR. The events can be changes on the existing user data, addition of user data, and so on. PCRF Server supports the Ud interface based on LDAP protocol, as defined in 3GPP TS 23.335 v9.x and TS 29.335 v9.x.

(viii) RADIUS Interface - PCRF Server provides a RADIUS based AAA interface which is connected with external AAA server. It receives the AAA-Start and AAA-Stop radius message forwarded from AAA server when IP-CAN session is established or terminated. It works with AAA management (component that provides the mapping between the IP Address and the MSISDN) to manage the mapping between IP address and MSISDN.

(ix) RADIUS CoA Interface – Radius Change of authorization (CoA) features provides a mechanism to change the attributes of an authentication, authorization and accounting (AAA) session after it is authenticated. When a policy changes for a user or user group in AAA, administrators can send the Radius CoA packets from the AAA server to reinitialize authentication and apply the new policy. PCRF Server also provides the connector and the processing flow used to provision policy rules to a non-3GPP enforcement point via RADIUS / RADIUS CoA interface.

(x) Gxx Interface – This reference point resides between the PCRF and the BBERF (Bearer Binding and Event Reporting Function). The Gxx reference point enables a PCRF to have dynamic control over the BBERF behavior. The PCRF PCC rule decisions may be based on information obtained from the BBERF via the Gxx interface. BBERF generally resides in the SGW.

(9) Call Flow with PCRF

9.1 In 2G/3G Network

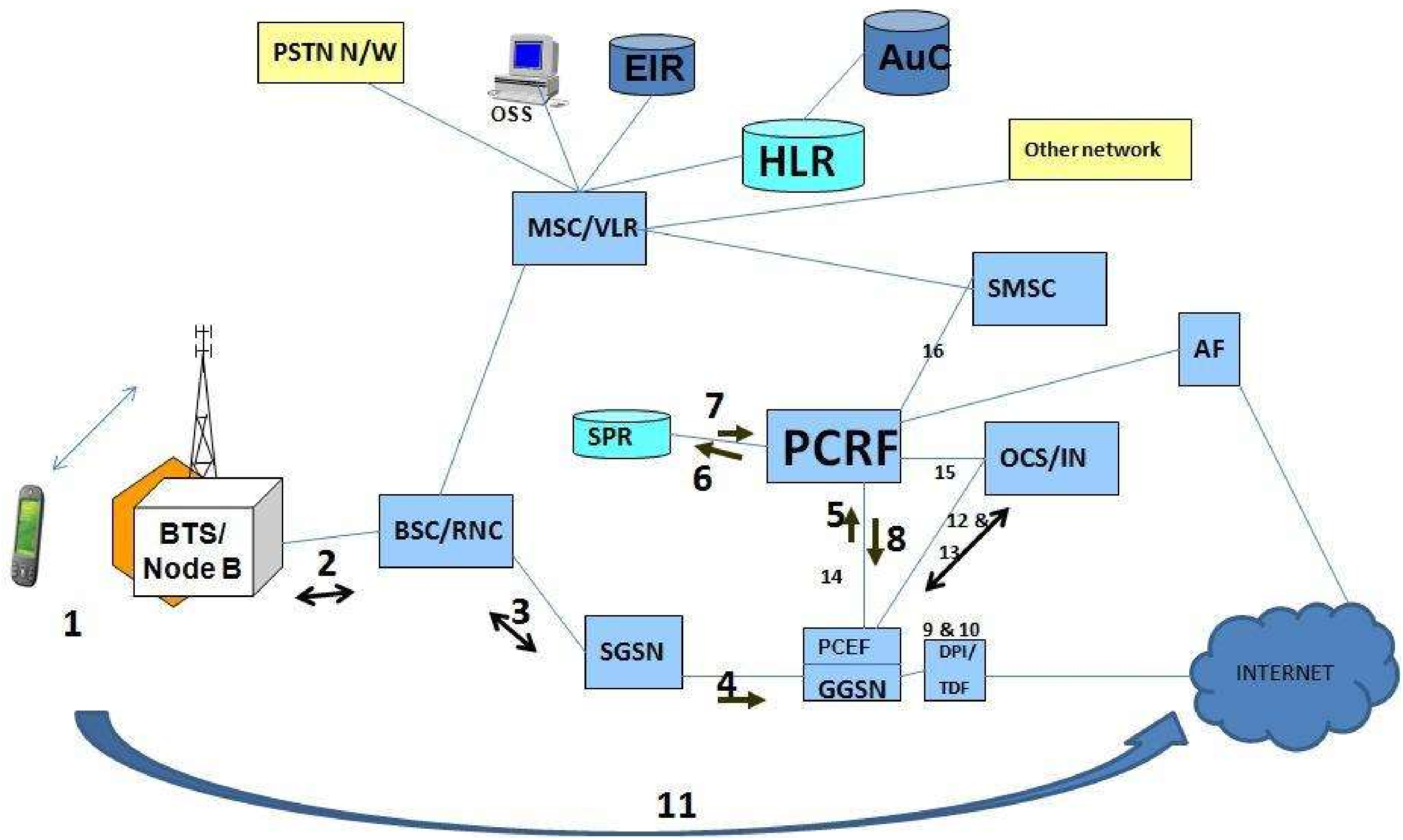


Figure 9.1: PCRF Call Flow in 2G/3G Network

Call Flow Procedures:

(1) User equipment (Mobile Station) wishes to establish a data application (data access/internet), so it requests to BTS/Node B.

(2) Node B forward its request to BSC/RNC.

(3) After all queries and procedure related to authentication, IMEI check & subscriber static information(HLR), BSC/RNC forward subscriber request to SGSN. Some of the queries are performed by SGSN.

(4) SGSN requests to GGSN for PDP context/data access.

(5) GGSN signals/query to PCRF (Policy & Charging Rule Function) about UE/MS data session establishment over Gx interface.

(6) PCRF queries the Subscriber Profile Repository(SPR) for dynamic information of subscriber over Sp interface.

(7) SPR sends all information about the subscriber policy/quota/rules to PCRF over Sp interface.

(8) PCRF installs policies for subscriber on GGSN (by PCEF) (per access point name[APN] and per bearer quota grants).

(9) If required, over Gx interface, Deep Packet Inspection(DPI) intimates PCRF on traffic detection. (Ud interface in the case of TDF [Traffic Detection Function])

(10) PCRF installs policies for application control on DPI and DPI begins tracking usage.

(11) Now data session is established and the subscriber starts consuming the data.

(12) Over Gy interface GGSN/PCEF talks to OCS (Online Charging System) for charging/credit.

(13) GGSN receives the information from OCS about balance/quota.

(14) GGSN signals policy server(PCRF) that device has exceeded data/quota grant or credit is low.

(15) Over Sy interface OCS also sends the credit limit report to PCRF.

(16) Policy server may grant additional grant, after consulting with subscriber by sending SMS notification over SMPP.

9.2 Call flow LTE EPC & PCRF

Network-Initiated IP-CAN Session Modification

9.2.1 Interactions between GW and PCRF (PCC Rule Provisioning in PUSH mode)

This flow shows the provisioning of PCC Rules and/or authorized QoS triggered by an event in the PCRF.

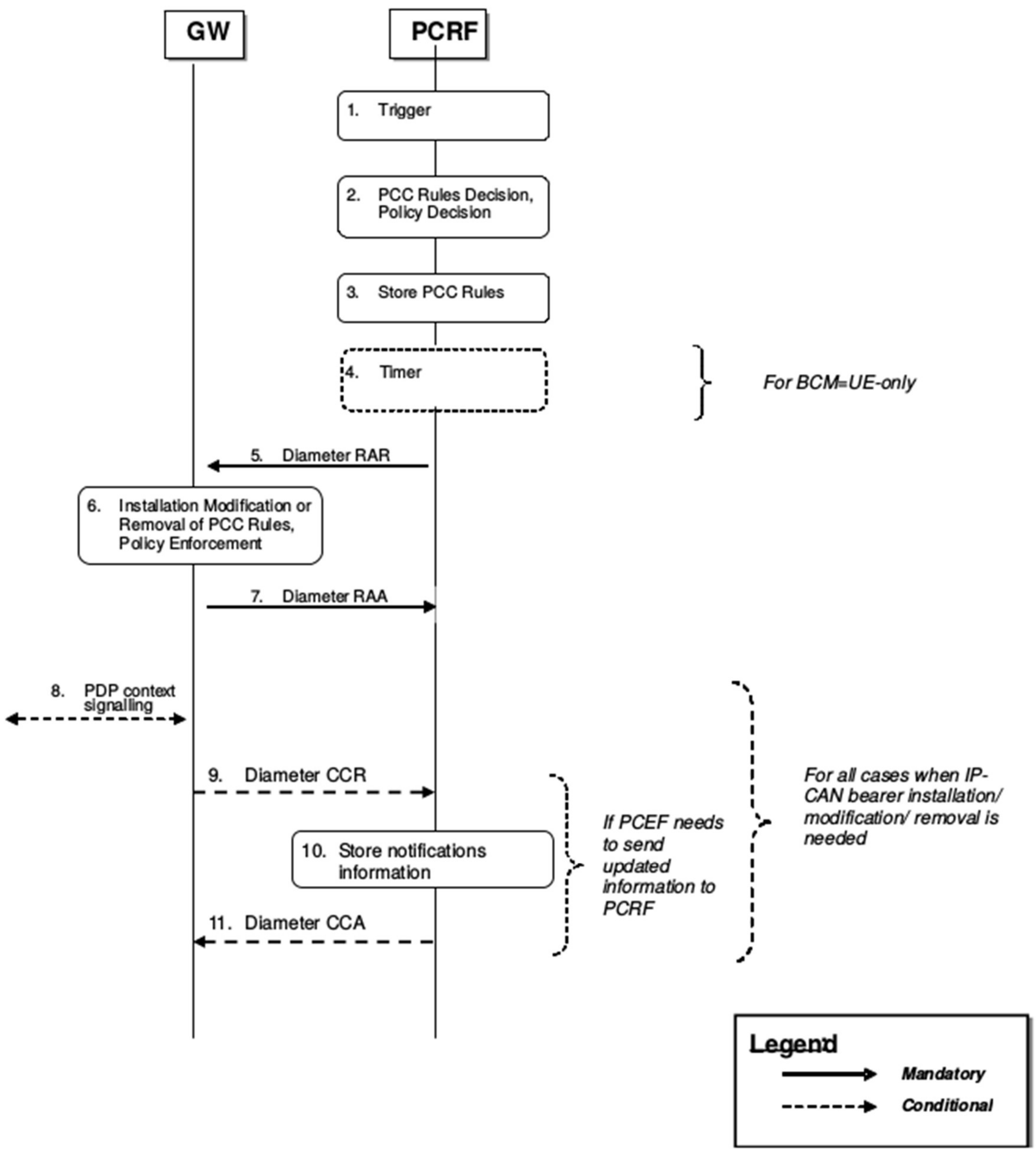


Figure 9.2.1: Interactions between GW and PCRF for PCRF-Initiated IP-CAN Session Modification

(1) The PCRF receives an internal or external trigger to re-evaluate PCC Rules and policy decision for an IP-CAN Session. Possible external trigger events are described in clause 9.2.1.

(2) The PCRF selects the PCC Rule(s) to be installed, modified or removed for the IP-CAN Session. The PCRF may also update the policy decision by defining an authorized QoS and enable or disable the service flow(s) of PCC Rules. If the PCEF controls the binding of IP-CAN bearers, PCRF may add or change QoS information per QCI applicable to that IP-CAN session.

(3) The PCRF stores the updated PCC Rules.

(4) Step 4 is only applicable if the Bearer Control Mode (BCM) selected is UE-only and the PCRF receives an external trigger from the AF.

The PCRF may start a timer to wait for an IP CAN bearer initiation, modification or removal procedure initiated by the UE, as depicted in figure 9.2.1 or figure 9.2.2 in the following cases:
- If the authorized QoS for an IP-CAN bearer is changed, or
- If One or more Flow Descriptions need to be added, deactivated or removed in any of the PCC rules bound to an IP-CAN bearer, or
- If as a result of policy decisions in step 2, new PCC rules need to be installed and the PCRF requires additional filter information from the UE to execute the bearer binding.

If an IP-CAN bearer initiation, modification or termination procedure initiated by the terminal is received for the affected PCC rules while the timer is running, all subsequent steps in the present figure shall not be executed and the steps in figure 9.2.1 or figure 9.2.2 (on provisioning based on PULL procedure at UE-initiated IP-CAN bearer establishment, modification or termination) shall be executed instead.

If the timer expires and the PCRF still requires additional filter information coming from the UE in order to decide on bearer binding for new PCC rules to be installed, all subsequent steps in the present figure shall not be executed, and further reactions of the PCRF are left unspecified. As a possible option, the PCRF could abort the AF session.
Otherwise, the PCRF shall proceed with the subsequent steps (provisioning based on PUSH procedure) in the present figure after timer expiry.

(5) The PCRF sends a Diameter RAR to request that the GW installs, modifies or removes PCC Rules and updates the policy decision.
For types of IP-CAN, where the PCRF controls IP-CAN Bearers, e.g. GPRS, the PCRF identifies the IP-CAN Bearer for each of the PCC Rules and the authorized QoS. The PCRF may provision PCC Rules and authorized QoS for several IP-CAN Bearers within the same RAR.

(6) The GW installs, modifies or removes the identified PCC Rules. The GW also enforces the authorized QoS and enables or disables service flow according to the flow status of the corresponding PCC Rules. If QoS information is received per QCI, PCEF shall set/update the upper limit for the MBR that the PCEF assigns to the non-GBR bearer for that QCI.

(7) The GW sends RAA to acknowledge the RAR. The PCEF informs the PCRF about the outcome of the PCC rule operation. If network initiated procedures apply for the PCC rule and the corresponding IP-CAN bearer cannot be established or modified to satisfy the bearer binding, then the PCEF rejects the activation of a PCC rule.

For GPRS, the subsequent steps are executed separately for each IP-CAN bearer under the following conditions:

- If all PCC rules bound to a PDP context have been removed or deactivated (PDP Context deactivation is applicable)
- If one or more PDP contexts have to be modified
- If in NW-Only Bearer Control Mode, the GGSN needs to establish a new PDP context (PDP Context establishment is applicable)

(8) For GPRS, the GGSN initiates the procedure to Create/Update or Terminate PDP Context Request message to the SGSN. If in the case of updating the PDP Context the authorized QoS for the bearer has changed, the GGSN will modify the UMTS QoS parameters accordingly.
When the procedure in step 8 is completed and requires of notifications from the GW to the PCRF the following steps are additionally executed:

(9) The GW sends the notifications needed to the PCRF. The notification is made by using a CCR messages with the needed AVPs. For an IP-CAN Bearer termination in UE-Only Bearer Control Mode, the GGSN sends a Diameter CCR with the Bearer-Identifier and Bearer-Operation AVPs to indicate "Termination".

(10) The PCRF stores the information coming in the notification.

(11) The PCRF acknowledge the CCR with a CCA command.

9.2.2 Interactions between PCRF, AF and SPR

AF Session Establishment

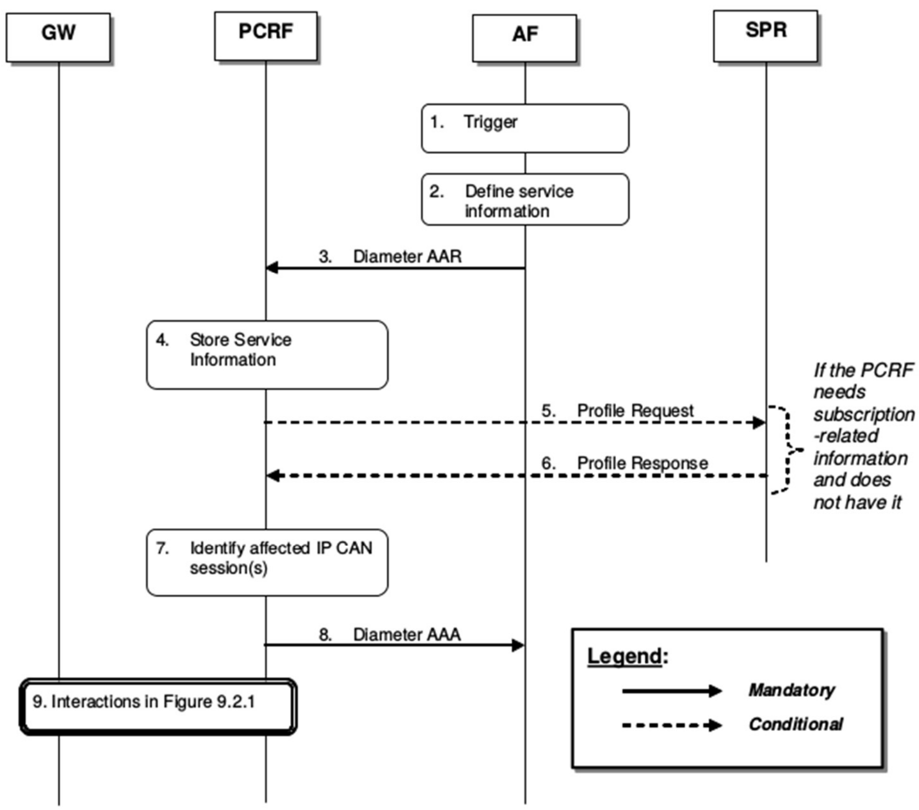


Figure 9.2.2: AF session establishment triggers PCRF-Initiated IP-CAN Session Modification

(1) The AF receives an internal or external trigger to set-up of a new AF session and provide Service Information.

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

(3) The AF provides the Service Information to the PCRF by sending a Diameter AAR for a new Rx Diameter session.

(4) The PCRF stores the received Service Information.

(5) If the PCRF requires subscription-related information and does not have it, the PCRF sends a request to the SPR in order to receive the information.

(6) The SPR replies with the subscription related information containing the information about the allowed service(s), QoS information and PCC Rules information.

NOTE:
For steps 5 and 6: The details associated with the Sp reference point are not specified in this Release. The SPR"s relation to existing subscriber databases is not specified in this Release.

(7) The PCRF identifies the affected established IP-CAN Session(s) using the information previously received from the GW and the Service Information received from the AF.

(8) The PCRF sends a Diameter AAA to the AF.

(9) The PCRF interacts with the GW according to figure 9.2.1.

(10) Advantages of Policy Server

In the intelligent network model, policy is the engine for innovation and differentiation. Its role evolves dramatically from its current usage, expanding both in application and scope.
To succeed as digital lifestyle providers, service providers require advanced tactics and tools that enable them to:

- Create a policy foundation that scales as the number of applications, use cases and network demands grow;
- Leverage network assets and analytics to gain a granular view of subscriber, application and network behavior from the handset to the core;
- Focus squarely on the subscriber with a rich service experience that’s tuned to each consumer’s behavior and provides direct personal benefit;
- Expand traditional, one-sided business models to engage and partner in new markets - machine-to-machine (M2M), over-the-top (OTT), mobile advertising, and cloud;
- Develop flexible, dynamic pricing strategies that address multiple market segments and offer end users more choices that reflect their usage patterns and lifestyles;

and

- Respond dynamically, often in real-time, to changing market and network dynamics.

With the ability to push policy control beyond the network core to its edge, operators can develop creative strategies to:

10.1 Optimize and personalize each subscriber's experience.

Operators can create a service experience that is related to each subscriber based on preferences, location, access network, device type, and network conditions. They can provide a relevant mobile advertisement, or inform the subscriber when a usage threshold is reached to prevent bill shock. Or, a service provider can zero rate social networking usage so it doesn't count against the subscriber's data bucket. Operators can offer service plans that guarantee bandwidth for certain high-value customers like corporate accounts, create flexible pricing plans that match a subscriber's preferences and budget, or allow subscribers to share one quota across multiple devices.

10.2 Create lucrative, two-sided business models with third-party, OTT and cloud providers.

Operators hold a number of valuable assets – QoS, security, billing relationships, subscriber profiles, context, usage, and device awareness – that can be used to create profitable commercial relationships. They can enable targeted third party advertising. Operators can offer identity as a service, enabling subscribers to use their network identity as a single-sign-on for third-party applications. Or, they can leverage the trusted relationship they've established with subscribers to provide secure, consolidated billing for OTT and cloud applications.

10.3 Maximize resources and Manage QoS.

Operators can implement creative solutions to manage network congestion. Advanced Wi-Fi offload use cases based on preferential network access, subscriber tier or type, device, application, quota, or network conditions can be implemented to relieve congestion on licensed spectrum and improve subscribers' data experience. A device can be moved to the best available network to ensure that the subscriber application usage receives the best available QoS based on current network conditions. The impact of high bandwidth applications can be minimized by offering subscribers incentives to shift their usage to a different time of day or less congested location. With advanced policy tools, operators can reduce the effect of the excessive signaling generated by "chatty" apps that constantly query the network.

(11) Conclusion

Policy and Charging Rules Function (PCRF) - supports service data flow detection, policy enforcement and flow-based charging. It offers a comprehensive solution that allows a new generation service provider to offer multiple use cases that allows them to better control their services and align their revenue with their resources.

PCRF Server provides a flexible and scalable software platform for the development and management of any type of policy solutions specialized for telecom industry. PCRF Server also offers flexibility in integration with various core network equipment or B/OSS systems using industry standard (e.g. 3GPP) or non-standard interfaces/protocols. PCRF Server enables the rapid prototyping and provisioning of new policies or products for innovative and unique services/applications to the subscribers.

As operators transition to LTE, policy will play a critical network role and become a strategic component in the quest to manage and monetize LTE networks. Virtually every LTE session and subscriber will need to be managed or charged in some fashion, which will require the involvement of a policy server in each transaction. From prioritization to personalized service plans, the coupling of LTE with policy promises to help resolve key LTE operational and business challenges and support a new generation of revenue generating services. Equipped with intelligent policy management, operators can shape and manage network demand, revenue contributions from differing classes of customers, capital expenditures, and overall growth of the LTE, mobile broadband market.

(12) GLOSSARY

3GPP: 3rd Generation Partnership Project
AF: Application Function
ATCA: Advanced Telecommunications Computing Architecture
BBERF: Bearer Binding and event reporting function
B/OSS: Business/Operations Support System
COTS: Commercial off the shelf
DCCA: Diameter Credit Control Application
DPI: Deep Packet Inspection
DSC: Diameter Signaling Controller
GGSN: Gateway GPRS Serving Node
IMS: IP Multimedia Subsystem
LDAP: Lightweight Directory Access Protocol
LTE: Long Term Evolution
OMC: Operation & Maintenance Center
OTT: Over the Top Platform
PCC: Policy & Charging Control
P-CSCF: Proxy Call Session Control Function
PCEF: Policy and Charging
PCRF: Policy & Charging Rule Function
PDF: Policy Decision Function
PGW: Packet Gate way
QoS: Quality of Service
SDN: Software Defined Network
SMS: Short Message Service
SMTP: Simple Mail Transfer Protocol
SMPP: Short Message Peer to Peer
SNMP: Simple Network Management Protocol
TDF: Traffic Detection Function
UDR: User Data Repository

(13) References

(1) ITU-T (www.itu.int/en/ITU-T)
(2) 3GPP (www.3gpp.org)
(3) ETSI (www.etsi.org)
(4) Policy Charging & Control Architecture (3GPP TS 23.203)
(5) Survey of Research Organization
(6) http://broabandtrafficmanagement.blogspot.in/p/dpi-market-size-forecast.html
(7) http://tec.gov.in/pdf/Studypaper/
(8) http://www.tutorialspoint.com/lte/lte_network_architecture.htm