Leveraging LTE PCC for Enhanced Services

Pradeep Bhardwaj
Technology Director – R&D
pradeep.bhardwaj@syniverse.com

Version .1

1. Introduction

Many operators are gearing up to embrace the standardization roadmap defined by 3GPP for the so-called 4G mobile technology to build on the technical foundations of the 3GPP family of cellular systems viz. GSM, GPRS, EDGE, WCDMA and HSPA as well as non-3GPP technologies viz. 1xRTT, EV-DO, 3xRTT. It is imperative that these operators expect the legacy systems, services and applications deployed already to evolve to support the LTE/SAE seamlessly along with the current breed of technologies. Also, as operators start deploying LTE/SAE in a phased manner, their expectations from the technology to be able to serve new breed of applications and services would grow as well.

With the emergence of innovative IP services, the transactional data usage is becoming more and more prevalent on the mobile. For example, the user downloads a purchased e-book from an online store, the user purchases and downloads a game from an operator store, the user views free trailer clip from an online library to determine whether to buy the entire movie or not. In many cases, the Sponsor (e.g. Application service provider) pays for the user's data usage in order to allow the user to access the Application Service Provider's services. This enables additional revenue opportunities for both the Application service providers and the operators.

In particular, such dynamic data usage provided by the Sponsor allows the operator to increase revenues from the users with limited data plans. The user may have limited data plans allowing only a nominal data volume per month and the Sponsor may dynamically sponsor additional volume for the user to allow access to the services offered by the Application service providers.

To cater to such use-cases, 3GPP has enhanced the PCC framework, in particular, allowing the operator to provide service control based on such sponsored services. For example, the PCC enhancements allow a dynamic IP flow to be excluded from the user's data plan since a Sponsor might sponsor the data usage for the identified IP flows. For example, the user may use the limited data plan to browse an online store for interested books; but once a book is purchased, the data usage for downloading the book can be granted for free. In addition, the IP flow may also be granted certain level of QoS (e.g. video streaming).

The objective of this white-paper is to provide a simplified understanding of the LTE/SAE PCC framework and capabilities as defined by 3GPP and to build upon this to understand how new/enhanced services can be created for mobile operators by fully leveraging the new capabilities introduced by 3GPP in its Release 11 specifications.

2. Overview of 3GPP PCC Framework

Let us start with an understanding of some of the basic terminology and concepts of PCC.

PCC (Policy Control & Charging)

The Policy and Charging Control (PCC) framework is used for QoS policy and charging control. It is optional for 3GPP EPS but needed if dynamic policy and charging control by means of PCC rules based on user and services are desired.

PCRF (Policy Control & Charging Rules Function)

PCRF is a functional element that encompasses policy control decision and flow based charging control functionalities. PCRF provides network control regarding the service data flow and application's traffic detection, gating, QoS and flow based charging (except credit management) towards the PCEF. The PCRF receives session and media related information from the AF and informs AF of traffic plane events. PCRF formulates the PCC Rule decisions based on information from various sources e.g. AF, PCEF, SPR.

PCEF (Policy Control Enforcement Function)

The PCEF is the functional element that encompasses policy enforcement and flow based charging functionalities. This functional entity is located at the Gateway (e.g. GGSN in the GPRS case, and PDG in the WLAN case). It provides control over the user plane traffic handling at the Gateway and its QoS, and provides service data flow detection and counting as well as online and offline charging interactions. For a service data flow that is under policy control the PCEF allows the service data flow to pass through the Gateway if and only if the corresponding gate is open.

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

Gx Interface

Gx is the Diameter interface between the PCRF and the PCEF. The PCRF acts as a Diameter Server whereas the PCEF acts as a Diameter Client. Gx enables a PCRF to have dynamic control over the PCC behaviour at a PCEF. The PCRF shall provision PCC Rules to the PCEF via the Gx reference point. Gx application uses VendorID 10415 (3GPP) and Application ID 16777238; included in Auth-Application-Id AVP. Diameter Agents can create route entry pointer to a different destination for Gx application. Some of the functions of the Gx interface are:

- Request for PCC decision from PCEF to PCRF
- Provision/Removal of PCC decision from PCRF to PCEF

- Delivery of IP-CAN-specific parameters from PCRF to PCEF or from PCEF to PCRF (relevant only when Gxx is deployed)
- Negotiation of IP-CAN bearer establishment mode (UE-only or UE/NW)
- Termination of Gx session (corresponding to IP-CAN session) by PCEF/PCRF
- Transmission of Traffic plane events from PCEF to PCRF.

Gx Interface Diameter Attributes:

Access-Network-Charging-Identifier-Gx	Event-Trigger	Precedence	QoS-Information
Allocation-Retention-Priority	Flow-Direction	Pre-emption-Capability	QoS-Negotiation
AN-GW-Address	Flow-Information	Pre-emption-Vulnerability	Qos-Upgrade
APN-Aggregate-Max-Bitrate-DL	Flow-Label	Priority-Level	Resource-Allocation-Notification
APN-Aggregate-Max-Bitrate-UL	IP-CAN-Type	Redirect-Information	Rule-Failure-Code
Bearer-Control-Mode	Guaranteed-Bitrate-DL	Redirect- Support	Security-Parameter-Index
Bearer-Identifier	Guaranteed-Bitrate-UL	Reporting-Level	TFT-Filter
Bearer-Operation	Maximum-Bandwidth	Routing-Filter	TFT-Packet-Filter-Information
Bearer-Usage	Max-Supported-Bandwidth-DL	Routing-IP-Address	ToS-Traffic-Class
Charging-Rule-Install	Max-Supported-Bandwidth-UL	Routing-Rule-Definition	Tunnel-Header-Filter
Charging-Rule-Remove	Metering-Method	Routing-Rule-Identifier	Tunnel-Header-Length
Charging-Rule-Definition	Monitoring-Key	Routing-Rule-Install	Tunnel-Information
Charging-Rule-Base-Name	Network-Request-Support	Routing-Rule-Remove	RAT-Type
Charging-Rule-Name	Offline	PCC-Rule-Status	Revalidation-Time
Charging-Rule-Report	Online	Session-Release-Cause	Rule-Activation-Time
Charging-Correlation-Indicator	Packet-Filter-Content	TDF-Information	Usage-Monitoring-Information
CoA-IP-Address	Packet-Filter-Identifier	TDF-Application-Identifier	Rule-DeActivation-Time
CoA-Information	Packet-Filter-Information	TDF-Destination-Host	Usage-Monitoring-Level
CSG-Information-Reporting	Packet-Filter-Operation	TDF-Destination-Realm	Usage-Monitoring-Report
Default-EPS-Bearer-QoS	Packet-Filter-Usage	TDF-IP-address	Usage-Monitoring-Support
Event-Report-Indication	PDN-Connection-ID	QoS-Class-Identifier	

Table-1: Gx Interface Diameter Attributes/AVPs.

Application Function (AF)

The AF is an element offering applications that require dynamic policy and/or charging control over the IP-CAN user plane behaviour. The AF communicates with the PCRF to transfer dynamic session information, required for PCRF decisions as well as to receive IP-CAN specific information and notifications about IP-CAN bearer level events. An example of an AF is the P-CSCF of the IM CN subsystem.

PCC Rules

PCC Rules are defined to:

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

There are 2 types of PCC Rules: Dynamic PCC Rules and Pre-defined PCC Rules. A PCC Rule consists of several attributes:

- Rule Name
- Service Identifier
- SDF filters
- Precedence
- Gate status
- QoS parameters
- Charging key
- Other Charging parameters.

3. 3GPP Release 11 New Functionality

3GPP Release 11 introduces a lot of changes and new functionality which overcomes some of the limitations/constraints of the current Gx reference model such that at any stage, for a subscriber there is only one PCRF-PCEF combination allowed for an IP service session, which limits the creation and control of new services outside the conventional PCRF-PCEF nodes.

New PCC Rule Attributes

3GPP Release 11 has added the following new attributes to the definition of a PCC Rule:

- Monitoring Key: The monitoring key for a PCC rule identifies a monitoring control instance that shall be used for usage monitoring control of the service data flows controlled by the predefined PCC rule or dynamic PCC rule.
- Sponsor Identity: If sponsored data connectivity is supported, the sponsor identity for a PCC rule identifies the 3rd party organization (the sponsor) willing to pay for the operator's charge for connectivity required to deliver a service to the end user.
- Application Service Provider Identity: If sponsored data connectivity is supported, the application service provider identity for a PCC rule identifies the 3rd party organization (the ASP) that is delivering the service to the end user.

New PCC Rule Criteria Input

3GPP Release 11 has added the possibility of a new input for the PCRF formulating its PCC Rule decisions:

- Information obtained from the TDF via the Sd reference point, e.g. report on application's traffic detection start/stop.

New Network Element TDF

3GPP Release 11 defines a new entity called TDF (Traffic Detection Function). The TDF allows Traffic shaping, Redirection, Gating & Bandwidth limitation for "detected" traffic.

New Network Interface Sd

3GPP Release 11 defines a new network interface or reference point called Sd between the PCRF and the TDF. This interface is used for:

- Establishment/termination of TDF session between PCRF and TDF
- Provisioning of Application Detection and Control rules from PCRF for traffic detection and enforcement at TDF

- Usage monitoring control of TDF session and of detected applications and reporting of start/stop of detected applications traffic and transfer of SDF descriptions for detected applications from TDF to PCRF.

New Feature on the PCEF

As an alternative to the TDF and the corresponding new Sd interface between the PCRF and the TDF, 3GPP Release 11 also defines a new feature called Application Detection & Control (ADC) for the PCEF. If permitted by the subscriber's profile configuration received from the SPR, the PCRF may invoke the application's traffic detection and control at the PCEF. If requested by PCRF, a PCEF, which supports Application Detection and Control feature, shall:

- Perform application's traffic detection and control
- Report the detected application's traffic start/stop events to the PCRF along with service flow descriptions, if available.

New PCC Extensions to enable Sponsored Connectivity

3GPP Release 11 introduced new procedures and extensions to support the Sponsored Connectivity concept, in particular:

- Providing to the PCRF via Rx reference point the identity of the Sponsor, the service data flows identifying the sponsored sessions, and optionally, the threshold limits for the sponsored sessions
- Enforcing sponsored connectivity rules at the PCEF based on monitoring key rules tied to sponsored connectivity
- Charging support for the sponsored connectivity sessions.

New Enhancements to Rx Reference Point for Sponsored Connectivity

3GPP Release 11 defines Rx reference point enhancements to allow transport of application level session information from AF to PCRF for usage control for service data flow. The PCRF needs to know the ASPs that have a business relationship with the operator and the policies that are related to them, primarily the QoS that is to be authorized for the sponsored IP flows. The PCRF may receive information about volume limits for service data flows from the AF. In order to enforce the volume limits for service data flow, the PCRF shall request usage report from the PCEF for the specified service data flows, provide the necessary usage threshold(s), and request the usage report triggers as needed. The PCRF shall notify the AF when usage threshold for the service data flow is reached. The amount of allowed resources (volume) received from the AF is independent of the overall allowed usage from the SPR. A service specific monitoring key is used for the usage reporting of volume limits received from the AF. The relative priority of the 3rd-Party Provider-Id (included in the profile) enables the PCRF to

differentiate among 3rd party providers when the total usage for all 3rd-party providers reaches a pre-determined level.

New Enhancements to Subscriber Profile Repository (SPR) for Sponsored Connectivity

In addition to the other information, the SPR will now also provide for a subscriber connecting to a specific PDN:

- 3rd-Party-Provider-ID, priority and list of applications
- Total usage per 3rd-Party Provider-Id and per application.

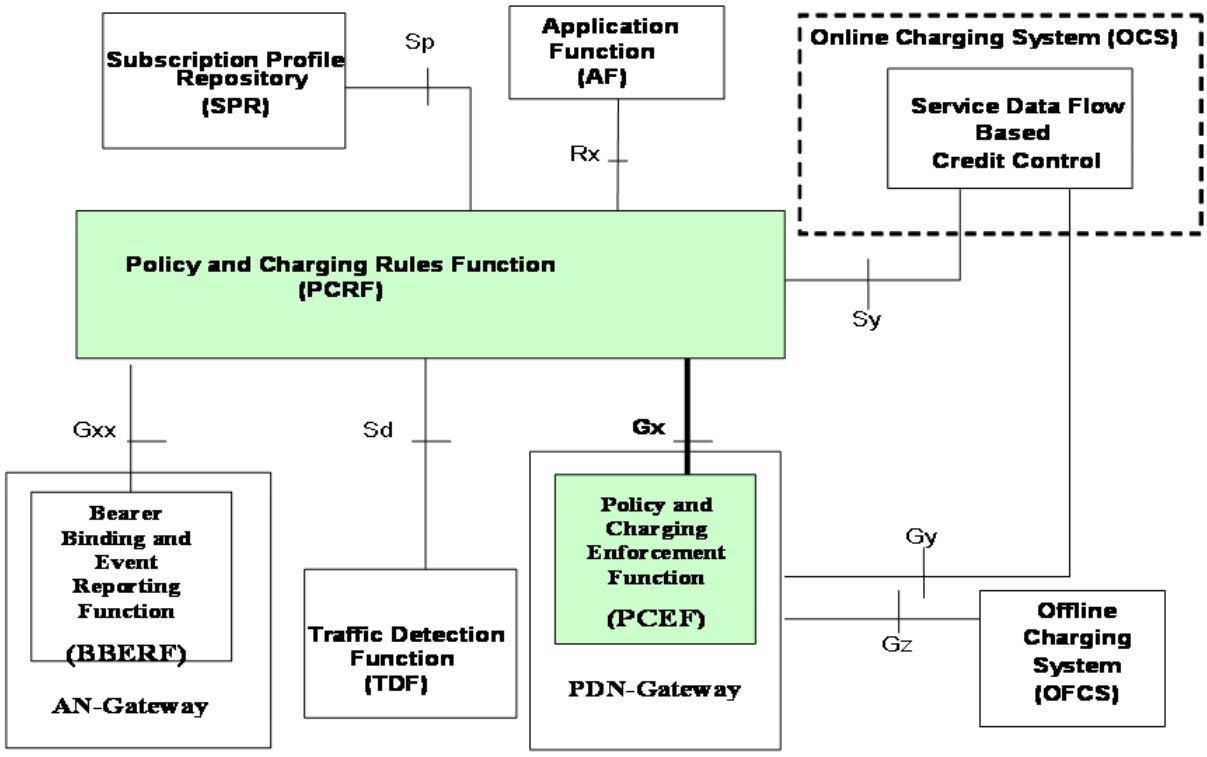

Figure-2: Gx/Sd Reference Model for PCC.

4. Usage Monitoring Control through the PCC

Usage monitoring may be performed for service data flows associated with one or more PCC rules. The provisioning of usage monitoring control per PCC rule is performed using the PCC rule provisioning procedure. For a PCRF-provided PCC rule, the monitoring key is set using the Monitoring-Key AVP within the Charging-Rule-Definition AVP of the PCC rule. For a predefined PCC rule, the monitoring key is included in the rule definition at the PCEF.

The PCRF may indicate, via the Gx reference point, the need to apply monitoring control for the accumulated usage of network resources on a per-IP-CAN session and user basis. Usage is defined as volume of user plane traffic. The data collection for usage monitoring control is performed per monitoring key, which may apply for a single Service Data Flow, a set of Service Data Flows or for all the traffic in an IP-CAN session.

If the PCRF requests usage monitoring control and if at this time, the PCRF is not subscribed to the "USAGE_REPORT" Event-Trigger, the PCRF includes the Event-Trigger AVP, set to the value "USAGE_REPORT", in a CC-Answer or RA-Request.

At IP-CAN session establishment and modification, the PCRF may provide the applicable thresholds for usage monitoring control to the PCEF, together with the respective monitoring keys. To provide the initial threshold for one or more monitoring key(s), the PCRF may include the threshold in either RA-Request or in the response of a CC-Request initiated by the PCEF.

During the IP-CAN session establishment, the PCRF may receive information about total allowed usage per PDN and/ or per UE from the SPR, i.e. the overall amount of allowed traffic volume that are to be monitored for the PDN connections of a user and/or total allowed usage for Monitoring key(s) per PDN and UE.

In order to provide the applicable threshold for usage monitoring control, the PCRF includes a Usage-Monitoring-Information AVP per monitoring key. The threshold level is provided in its Granted-Service-Unit AVP. Threshold levels may be defined for:

- the total volume only, or
- the uplink volume only, or
- the downlink volume only, or
- the uplink and downlink volume.

The PCRF provides the applicable threshold(s) in the CC-Total-Octets, CC-Input-Octets or CC-Output-Octets AVPs of the Granted-Service-Unit AVP. The monitoring key is provided in the Monitoring-Key AVP. The PCRF may provide multiple usage monitoring control instances. The PCRF indicates if the usage monitoring instance applies to the IP-CAN session or to one or more PCC rules. For this purpose, the Usage-Monitoring-Level AVP may be provided with a value respectively set to SESSION_LEVEL or

PCC_RULE_LEVEL. The PCRF may provide one usage monitoring control instance applicable at IP-CAN session level and one or more usage monitoring instances applicable at PCC Rule level.

If the PCRF wishes to modify the threshold level for one or more monitoring keys, the PCRF provides the thresholds for all the different levels applicable to the corresponding monitoring key(s).

If the PCRF wishes to modify the monitoring key for the session level usage monitoring instance, it disables the existing session level monitoring usage instance and provides a new session level usage monitoring instance. The PCRF may enable the new session level usage monitoring instance and disable the existing session level usage monitoring instance in the same command.

When the accumulated usage is reported in a CCR command, the PCRF indicates to the PCEF if usage monitoring shall continue for that IP-CAN session, usage monitoring key, or both as follows:

- If monitoring shall continue for specific level(s), the PCRF provides the new thresholds for the level(s) in the CC-Answer using the same AVP as before (CC-Total-Octets, CC-Input-Octets or CC-Output-Octets AVP within the Granted-Service-Unit AVP);
- otherwise, if the PCRF wishes to stop monitoring for specific level(s) the PCRF won't include an updated usage threshold in the CCA command for the stopped level(s) i.e. the corresponding CC-Total-Octets, CC-Input-Octets or CC-Output-Octets AVPs shall not be included within Granted-Service-Units AVP.

When usage monitoring is enabled, the PCRF may request the PCEF to report accumulated usage for one or more enabled monitoring keys regardless if a usage threshold has been reached by sending to the PCEF within the Usage-Monitoring-Information AVP the Usage-Monitoring-Report AVP set to the value USAGE_MONITORING_REPORT_REQUIRED. The PCRF only requires PCEF to report accumulated usage for one or more monitoring keys in a CC-Answer when the PCEF has not provided accumulated usage in the CC-Request for the same monitoring key(s).

To specify the usage monitoring key for which usage is requested the PCRF includes the usage monitoring key within the Monitoring-Key AVP within the Usage-Monitoring-Information AVP. To request usage be reported for all enabled usage monitoring keys the PCRF omits the Monitoring-Key.

The PCRF processes the usage reports and performs the actions as appropriate for each report.

5. Reporting Accumulated Usage by the PCEF

When usage monitoring is enabled, the PCEF measures the volume of the IP-CAN session or the volume of the applicable service data flows and reports accumulated usage to the PCRF in the following conditions:

- when a usage threshold is reached
- when all PCC rules for which usage monitoring is enabled for a particular usage monitoring key are removed or deactivated
- when usage monitoring is explicitly disabled by the PCRF
- when an IP-CAN session is terminated
- when requested by the PCRF.

To report accumulated usage for a specific monitoring key the PCEF sends a CC-Request with the Usage-Monitoring-Information AVP including the accumulated usage since the last report. For each of the enabled monitoring keys to be reported, the Usage-Monitoring-Information AVP includes the monitoring key in the Monitoring-Key AVP and the accumulated volume usage in the Used-Service-Unit AVP. Accumulated volume reporting is done for the total volume, the uplink volume or the downlink volume as requested by the PCRF, and set in CC-Total-Octets, CC-Input-Octets or CC-Output-Octets AVPs of Used-Service-Unit AVP respectively. The PCEF continues to perform volume measurement after the report until instructed by the PCRF to stop the monitoring.

For cases where the PCRF indicates in a CC-Answer command whether the usage monitoring shall continue as a response to the reporting of accumulated usage in a CCR command, the PCEF behaves as follows

- if the PCRF provisions an updated usage threshold in the CCA command, the monitoring continues using the updated threshold value provisioned by the PCRF;
- otherwise, if the PCRF does not include an updated usage threshold in the CCA command, the PCEF does not continue usage monitoring for that IP-CAN session, usage monitoring key, or both as applicable.

Upon receiving the reported usage from the PCEF, the PCRF deducts the value of the usage report from the total allowed usage for that IP-CAN session, usage monitoring key, or both as applicable, and the PCRF may also derive the PCC rules based on the remaining allowed usage or reported usage and provision them to the PCEF.

5.1 Usage Threshold Reached

When usage monitoring is enabled for a particular monitoring key, the PCEF measures the volume of all traffic for the IP-CAN session or the corresponding service data flows and notifies the PCRF when a

usage threshold for that monitoring key is reached and reports the accumulated usage for that monitoring key and includes the "USAGE_REPORT" Event-Trigger in a CCR command with CC-Request Type AVP set to the value "UPDATE_REQUEST" by following the procedures to report accumulated usage at the service data flow level.

5.2 PCC Rule Removal

When the PCRF removes or deactivates the last PCC rule associated with a usage monitoring key in an RAR or CCA command in response to a CCR command not related to reporting usage for the same monitoring key, the PCEF sends a new CCR command with the CC-Request-Type set to the value "UPDATE_REQUEST" including the Event-Trigger set to "USAGE_REPORT" to report accumulated usage for the usage monitoring key within the Usage-Monitoring-Information AVP using the procedures to report accumulated usage at the service data flow level.

When the PCEF reports that the last PCC rule associated with a usage monitoring key is inactive, the PCEF reports the accumulated usage for that monitoring key within the same CCR command if the Charging-Rule-Report AVP was included in a CCR command; otherwise, if the Charging-Rule-Report AVP was included in an RAA command, the PCEF sends a new CCR command to report accumulated usage for the usage monitoring key.

5.3 Usage Monitoring Disabled

Once enabled, the PCRF may explicitly disable usage monitoring as a result of receiving a CCR from the PCEF which is not related to reporting usage, other external triggers (e.g., receiving an AF request, subscriber profile update), or a PCRF internal trigger. When the PCRF disables usage monitoring, the PCEF reports the accumulated usage which has occurred while usage monitoring was enabled.

To disable usage monitoring for a monitoring key, the PCRF sends the Usage-Monitoring-Information AVP including only the applicable monitoring key within the Monitoring-Key AVP and the Usage-Monitoring-Support AVP set to USAGE_MONITORING_DISABLED.

When the PCRF disables usage monitoring in a RAR or CCA command, the PCEF sends a new CCR command with CC-Request Type AVP set to the value "UPDATE_REQUEST" and the Event-Trigger AVP set to "USAGE_REPORT" to report accumulated usage for the disabled usage monitoring key(s).

5.4 IP-CAN Session Termination

At IP-CAN session termination the PCEF sends the accumulated usage information for all monitoring keys for which usage monitoring is enabled in the CCR command with the CC-Request-Type AVP set to the value "TERMINATION_REQUEST" using the procedures to report accumulated usage.

If all IP-CAN sessions of a user to the same APN are terminated, the PCRF may store the remaining allowed usage, i.e. the information about the remaining overall amount of resources, in the SPR.

5.5 PCRF Requested Usage Report

When the PCEF receives the Usage-Monitoring-Information AVP including the Usage-Monitoring-Report AVP set to the value USAGE_MONITORING_REPORT_REQUIRED, the PCEF sends a new CCR command with CC-Request Type AVP set to the value "UPDATE_REQUEST" and the Event-Trigger AVP set to "USAGE_REPORT" to report accumulated usage for the monitoring key received in the Usage-Monitoring-Information AVP using the procedures to report accumulated usage. If the Monitoring-Key AVP was omitted in the received Usage-Monitoring-Information AVP, the PCEF sends the accumulated usage for all the monitoring keys that were enabled at the time the Usage-Monitoring-Information was received.

Feature bit	Feature	M/O	Description
0	Rel8	M	This feature indicates the support of base 3GPP Rel-8 Gx functionality, including the AVPs and corresponding procedures supported by the base 3GPP Rel-7 Gx standard, but excluding those features represented by separate feature bits.
1	Rel9	M	This feature indicates the support of base 3GPP Rel-9 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 feature bit, but excluding those features represented by separate feature bits.
2	ProvAFsignalFlow	O	This feature indicates support for the feature of IMS Restoration. If PCEF supports this feature the PCRF may provision AF signaling IP flow information.
3	Rel10	M	This feature indicates the support of base 3GPP Rel-10 Gx functionality, including the AVPs and corresponding procedures supported by the Rel8 and Rel9 feature bit, but excluding those features represented by separate feature bits.
4	SponsoredConnectivity	O	This feature indicates support for sponsored data connectivity feature. If the PCEF supports this feature, the PCRF may authorize sponsored data connectivity to the subscriber.
5	IFOM	O	This feature indicates support for IP flow mobility feature.
6	ADC	O	This feature indicates support for the Application Detection and Control feature.

Table-2: Features of Feature-List-ID 1 used in Gx.

6. Sponsored Data Connectivity through the PCC

With sponsored data connectivity, the sponsor has a business relationship with the operator and pays the operator for user's connectivity in order to allow the user access to services provided by the sponsor, a 3rd party service provider or the operator. Alternatively the user pays for the connectivity with a transaction which is separate from the subscriber's online charging. It is assumed the user has already a subscription with the mobile operator.

The following actors are involved in a scenario of sponsored connectivity:

- Sponsor – the party willing to take the operator's charge for connectivity.
- Service provider – the party providing the sponsored service (may be the same as the sponsor).
- Operator – the party providing connectivity (may also be service provider).
- End user – the one using the sponsored service (is a subscriber of the operator).

There are two scenarios for the ASP possible: the ASP is only involved in the application level signaling or the ASP is in addition involved in the user data exchange, i.e. the IP packets carrying the payload of the application.

Sponsored data connectivity may be performed for service data flows associated with one or more PCC rules if the information about the sponsor, the application service provider and optionally the threshold values are provided by the AF.

The provisioning of sponsored data connectivity per PCC rule is performed using the PCC rule provisioning procedure. The sponsor identity is set using the Sponsor-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. The application service provider identity is set using the Application-Service-Provider-Identity AVP within the Charging-Rule-Definition AVP of the PCC rule. Sponsor-Identity AVP and Application-Service-Provider-Identity AVP are included if the Reporting-Level AVP is set to the value SPONSORED_CONNECTIVITY_LEVEL.

When receiving the flow based usage thresholds from the AF, the PCRF uses the sponsor identity to generate a monitoring key. The PCRF may also request usage monitoring control following the procedure specified in section 4, in this case, only the flow based usage is applied for the sponsored data connectivity. If requested, the PCEF may also report the usage to the PCRF following the procedure specified in section 5.

6.1 Call Flow for Sponsored Data Connectivity Rule

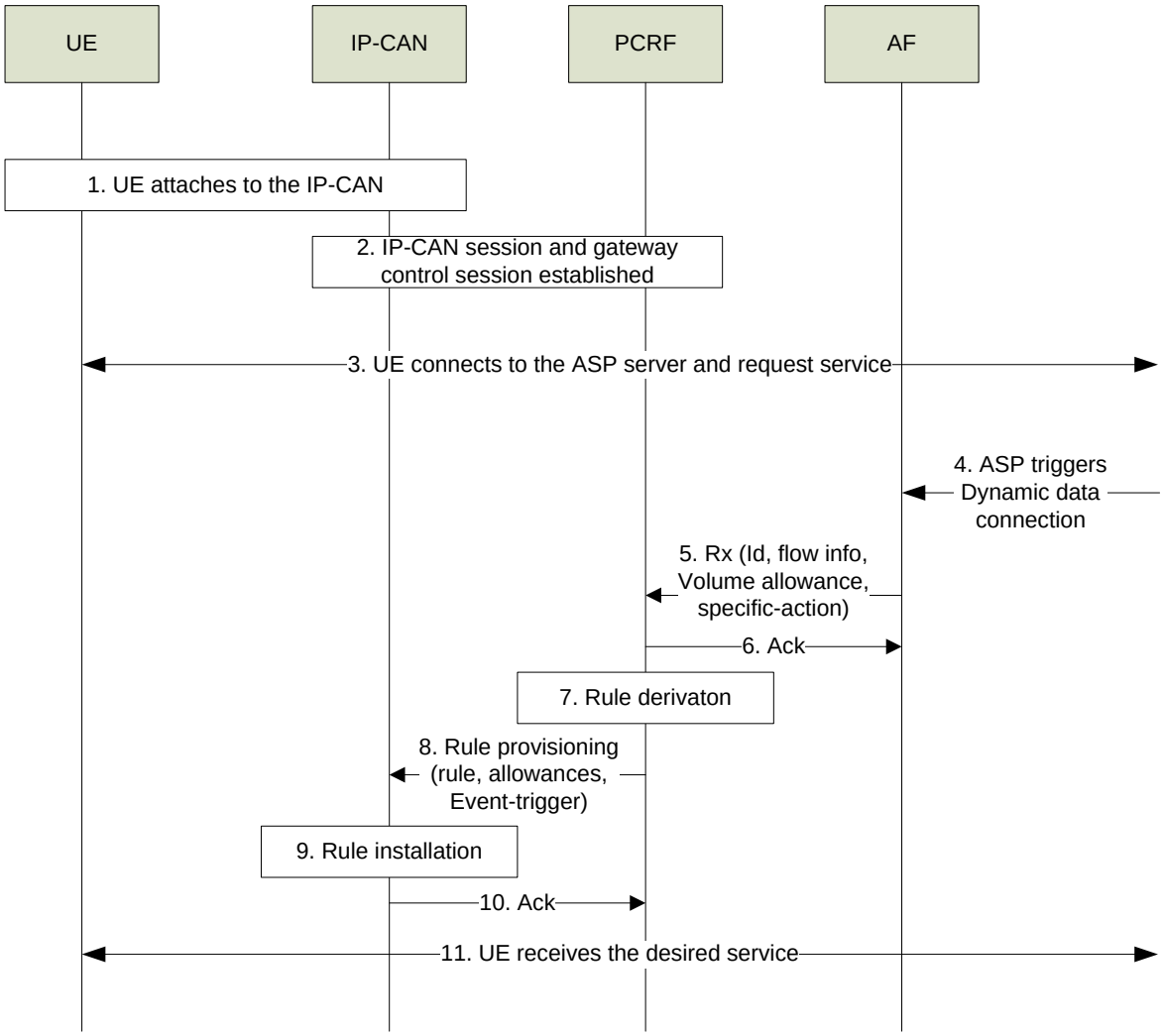

Figure-3: Call flow for sponsored data connectivity rule installation.

1. The UE attaches to the IP-CAN following the normal procedures specific to the IP-CAN.
2. The PCEF establishes IP-CAN session and/or gateway control session towards the PCRF. The UE's IP connection may have a limited amount of data usage.
3. The UE connects to the 3rd party ASP server and requests services from the ASP.
4. The ASP server decides to sponsor the data connection used to access the ASP service for the user and provide dynamic sponsoring information to the AF within the operator's network. The dynamic sponsoring information includes the user identity to be sponsored (e.g. the IP address), the IP flow information to be sponsored, the usage amount to be sponsored and the threshold request related to the sponsored data connectivity.

5. For each sponsored data connectivity required, the AF establishes an Rx session towards the PCRF and provides the identity of the 3rd party ASP and 3rd party Application-Function-ID, the user identity and the service information optionally including volume allowance and specific-actions related to the service.
6. The PCRF authorizes and acknowledges the service information received from the AF.
7. The PCRF derives PCC/QoS rules related to the sponsored data connectivity, and may take into account 3rd party Provider priority, total usage limit per 3rd-Party Provider-Id, and 3rd party Application-ID, and total usage limits of all 3rd parties.
8. The PCRF provision the rules and event triggers for the sponsored data connectivity to the PCEF.
9. The PCEF installs the provisioned rules and event triggers.
10. The PCEF sends acknowledgement to the PCRF.
11. The UE uses the sponsored connectivity to receive the desired service from the ASP.

7. Conclusions

The 3GPP PCC framework and the associated, new functionality introduced in 3GPP Release 11 provides a very flexible, standardized and future-proof mechanism for implementation of new/enhanced services e.g. Sponsored Data Access, Roaming monitoring & control of services.

References:

1. 3GPP TS 29.215 V11.1.0
2. 3GPP WID SP-110196
3. 3GPP TR 23.813
4. 3GPP TS 23.203

About the Author

Pradeep Bhardwaj is currently Technology Director – R&D at Syniverse Technologies, based in the United Kingdom and is a senior technology advisor providing consulting and direction on the subjects of emerging technologies and trends including all LTE matters within the organization and for its clients. Until recently, he was also the Chairman of the GSMA Hubbing Provider Interworking Group (HPIG) from beginning to end. He is a recognized industry expert with over 20 years of experience with mobile operators and telcos in the areas of 2G/3G, LTE, IMS, International Roaming, Satellite & Data communications. He can be reached at Pradeep.bhardwaj@syniverse.com.