**Policy and Charging Rules Function Node**

***Project report submitted in partial fulfillment of the requirement for the degree of***

***Bachelor of Technology in Computer Science Engineering***

**Submitted by**

**Sarthak Roy (1121028)**

**Under the Supervision of**

**Sudhanshu Garg**

**Navitha Thakur**

**Akshay Jain**

****

**SCHOOL OF COMPUTER SCIENCE ENGINEERING**

**KIIT UNIVERSITY**

**BHUBANESWAR-751024**

**2015**

**CERTIFICATE**

This is to certify that “Sarthak Roy” has carried out the Project work entitled “Policy and Charging Rules Function” for the award of Bachelor of Technology Degree in Computer Science from KIIT University, Bhubaneswar, India.

To the best of our knowledge, this work has not been submitted earlier to any university for the award of any degree.

***Sudhanshu Garg***

***(Senior Project Manager)***

***(Aricent Technologies)***

***Akshay Jain***

***(Mentor)***

***(Aricent Technologies)***

***Bhabani Shankar Prasad Mishra***

***(Associate Dean)***

**ACKNOWLEDGMENT**

I take this opportunity to express my sincere gratitude to my supervisors Sudhanshu Garg, Navitha Thakur and Akshay Jain for their invaluable guidance. It would have never been possible for me to take this project to completion without their innovative ideas and their relentless support and encouragement. It has been a very enlightening experience to work under them.

We are also grateful to Prof. Samaresh Mishra, Dean of School of Computer Engineering, for his constant inspiration and encouragement during our work. We would also like to thank all faculty members of Department of Computer Engineering for their invaluable knowledge they imparted to us and for teaching the principles in an exciting and enjoyable way.

Our special thanks to my friends for their constant suggestions in my work and moral boost. I thank all staff members of School of Computer Engineering of KIIT University who helped in many ways directly or indirectly during the period of our work.

We express my deep sense of reverence and gratitude to our parents, for their love, concern and blessings which are always with us.

Sarthak Roy

**Abstract**

Policy and Charging Rules Function (PCRF) is a function within the evolved packet core network of the telecommunications infrastructure and systems. PCRF enables policy rules making through the aggregation of information to and from the network, comprising components such as operational support systems, business support systems, subscriber management platforms, usage databases and other systems which are executed in real-time, supporting policy decisions at both the network level and also at the subscriber level. The Diameter base protocol is intended to provide an Authentication, Authorization and Accounting (AAA) framework for applications such as network access or IP mobility. Diameter is also intended to work in both local Authentication, Authorization & Accounting and roaming situations. The Diameter base application needs to be supported by all Diameter implementations.

*Key words*—

AF: Application Function

BBERF: Bearer Binding and Event Reporting Function

BBF: Bearer Binding Function

DRA: Diameter Routing Agent

H-PCEF: A PCEF in the HPLMN

H-PCRF: A PCRF in the HPLMN

HRPD: High Rate Packet Data

HSGW: HRPD Serving Gateway

IP-CAN: IP Connectivity Access Network

OFCS: Offline Charging System

OCS: Online Charging System

PCC: Policy and Charging Control

PCEF: Policy and Charging Enforcement Function

PCRF: Policy and Charging Rules Function

QCI: QoS Class Identifier

SPR: Subscription Profile Repository

Contents

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | 1. Introduction | 7 | | 1.1 *Introduction PCRF* | 7 | | 1.2 *Introduction Diameter* | 10 | | 2. PCRF and Diameter working | 11 | | 2.1 *Interfaces used for PCRF* | 11 | | 2.2 *Diameter messages for PCRF* | 12 | | *2.2.1 PCC rules on Gx* | 13 | | *2.2.2 Rx Messages* | 22 | | *2.2.3 Diameter application for Sh interface* | 26 | | 3. Result Codes | 32 | | 4. Conclusions | 34 | | References | 35 | |  |

**Chapter 1**

**Introduction**

* 1. ***Introduction PCRF***

PCRF is a node placed in the EPC of LTE network. As a policy engine, it performs the following functions:

•Flow Based Charging, including charging control and online credit control.

•Policy control (for example. gating control, QoS control, QoS signaling) PCRF enables us to control policies and QoS in real time network.

The PCRF controls bandwidth or usage while communicating with other peer nodes and when the network is busy, it enables network operators:

•To offer high quality of services to the user.

•To offer precise pricing plans to the user PCRF supports three interfaces that are Gx Interface, Sh Interface, and Rx Interface.

Following features are supported in PCRF release 2.1:

•System Features

The system features helps you to control and monitor the PCRF. It also helps in enhancing the performance of the PCRF.PCRF supports the following system features:

−Starting PCRF

−System Dashboard

−Multiple Operator Group

−Scalable PCRF

−Fault management

−Monitoring Network

−Deployment Configuration

−Peer Discovery

−PCRF Restoration

−SMP Support

−64 Bit support

−High Availability (HA)

−IPv6 Support

•Policy Engine Features

The policy engine features helps you to control and monitor the policy derivation and charging mechanism in PCRF. The following are the user customizable policy engine features:

−Trigger Based Policy Selection

−Deep Packet Inspection (DPI) Engine Support

−Location Based Policy

−Time Based Policy

−Event Based Policy

−Subscriber Type Based Policy

−Subscriber Based Policy

−Application Based Dynamic Policy

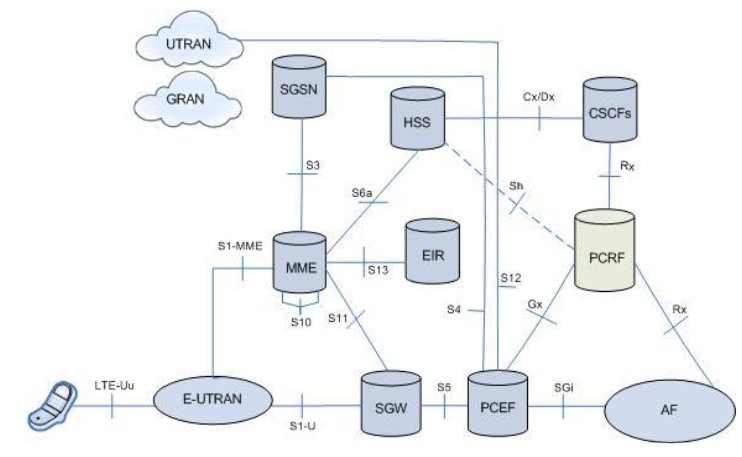
−IMS Call Policy

−Service Based Policy

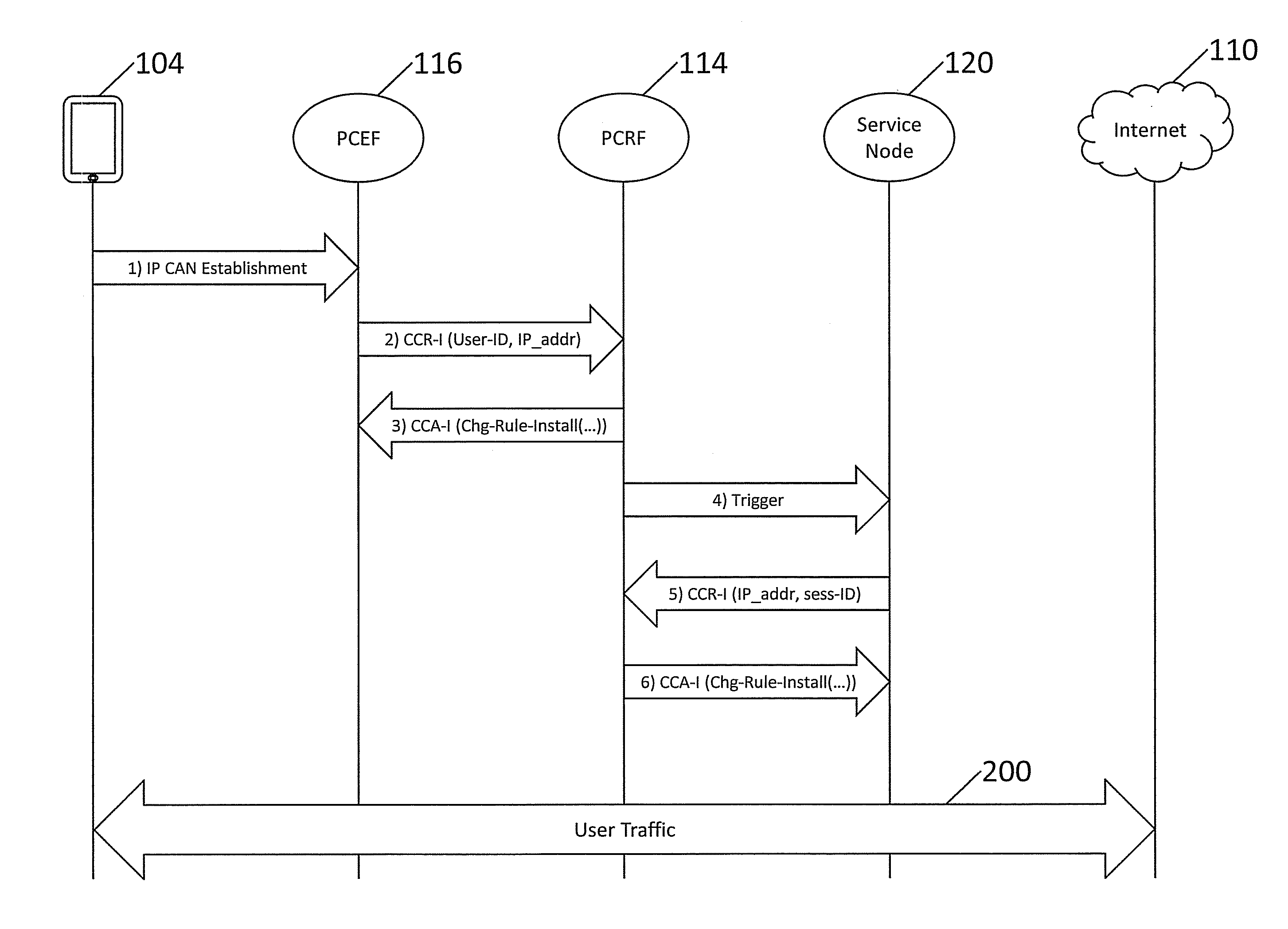
−Access Network Type Based Policy

−Usage Based Policy

−Policy Based Charging Control

******

***Positioning of PCRF node in LTE-EPC***

******

***Message flow***

***1.2 Introduction DIAMETER***

Diameter protocol was derived from the RADIUS protocol. It is an IP based signaling protocol for Advanced telecom networks. It is a message based protocol as all the communication between different diameter nodes takes place through message exchanges .It is a message based protocol as all the communication between different diameter nodes takes place through message exchanges .It Supports Failover and Failback Procedures. The host who implements the diameter protocol called DIAMETER Node. DIAMETER is designed as a Peer-To-Peer architecture means act as either a client or a server depending on network deployment. DIAMETER node is used to refer to a Diameter client, a Diameter server, or a Diameter agent.

**Chapter 2**

**PCRF and Diameter working**

**2.1 Interfaces used for PCRF**

PCRF supports the following standard and product interfaces to communicate with the other LTE nodes, 3G nodes, and third party entities:

**Standard Interfaces**

To enable its communication with the other LTE nodes, such as, PCEF, HSS, and AF, PCRF supports the following interfaces:

• **Gx interface**

The Gx interface resides between the PCRF and the PCEF. It performs the following functions:

−Provisioning and removing of PCC rules from the PCRF to the PCEF.

−Transmitting traffic plane events from the PCEF to the PCRF.

−Charging control, policy control or both by applying AVPs relevant to the application.

**• Sh interface**

The Sh interface resides between the PCRF and the HSS. It enables PCRF to request the subscription information related to the subscriber from the HSS. PCRF receives this information based on the subscriber ID in the form of Mobile Station Integrated Services Digital Network (MSISDN).

**• Rx interface**

An Rx interface is used to exchange application level session information between the PCRF and the AF. The PCRF uses this information for the PCC decisions. The information are:

−IP filter information to identify the service data flow for policy control and/or to differentiated charging.

−Media/application bandwidth requirements for QoS control.

**Product Interfaces**

For configuration, monitoring, and event or alarm reporting, PCRF provides the C structure API interface to the 3rd party management entity.



*Interfaces of PCRF*

**2.2 Diameter messages for PCRF**

All data delivered by the protocol is in the form of an AVP. Some of these AVP values are used by the Diameter protocol itself, while others deliver data associated with particular applications that

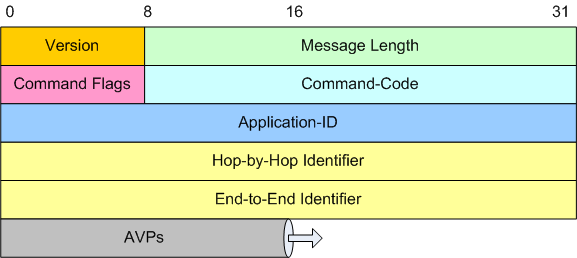
employ Diameter. AVPs may be added arbitrarily to Diameter messages, so long as the required AVPs are included and AVPs that are explicitly excluded are not included. AVPs are used by the base.Diameter protocol to support the following required features:

- Transporting of user authentication information, for the purposes of enabling the Diameter server to authenticate the user.

- Transporting of service specific authorization information, between client and servers, allowing the peers to decide whether a user’s access request should be granted.

- Exchanging resource usage information, which MAY be used for accounting purposes, capacity planning, etc.

- Relaying, proxying and redirecting of Diameter messages through a server hierarchy.



*Diameter Header*

### **2.2.1 PCC Rules on Gx**

The purpose of the PCC rule is to:

- Detect a packet belonging to a service data flow.

- The service data flow filters within the PCC rule are used for the selection of downlink IP CAN bearers.

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

- Identify the service the service data flow contributes to.

- Provide applicable charging parameters for a service data flow.

- Provide policy control for a service data flow.

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

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

- Dynamic PCC rules. Dynamically provisioned by the PCRF to the PCEF via the Gx interface. These PCC rules may be either predefined or dynamically generated in the PCRF. Dynamic PCC rules can be installed, modified and removed at any time.

- Predefined PCC rules. Preconfigured in the PCEF. Predefined PCC rules can be activated or deactivated by the PCRF at any time. Predefined PCC rules within the PCEF may be grouped allowing the PCRF to dynamically activate a set of PCC rules over the Gx reference point.

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

A PCC rule consists of:

- A rule name;

- Service identifier;

- Service data flow filter(s);

- Precedence;

- Gate status;

- QoS parameters;

- charging key (i.e. rating group);

- Other charging parameters;

- monitoring key;

- sponsor identity;

- Application service provider identity.

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

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

The service flow filter(s) shall be used to select the traffic for which the rule applies. It shall be possible to define wild carded service data flow filter(s), both for the dynamic and predefined PCC rules.

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

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

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

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

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

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.

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.

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.

### **Operations on PCC Rules**

For dynamic PCC rules, the following operations are available:

- Installation: to provision a PCC rules that has not been already provisioned.

- Modification: to modify a PCC rule already installed.

- Removal: to remove a PCC rule already installed.

For predefined PCC rules, the following operations are available:

- Activation: to allow the PCC rule being active.

- Deactivation: to disallow the PCC rule.

**Capability Negotiation**

The basic motive of this process is to KNOW about the other node to which a node intended to communicate before establishing the connection, i.e. whether other node contains the applications for which node wants to communicate.

Technically speaking, It is the process where two diameter peer exchange their identity and its capabilities (such as protocol version number, supported diameter applications, security mechanism etc.). Peer share their capabilities by CER/CEA Message (Capability-Exchange-Request/Capability-Exchange-Answer).  
  
If one peer sends a CER message to another Peer and receiver does not have support for

1) Any common application then it must return the CEA with Result-Code Avp set to DIAMETER\_NO\_COMMON\_APPLICATION and should disconnect the transport layer connection.  
  
2) No common security mechanism then it must return the CEA with Result-Code Avp set to DIAMETER\_NO\_COMMON\_SECURITY and should disconnect the transport layer connection. (Only maintained to have backward compatibility Because in latest release Transport Level security is establish before diameter connection so CER/CEA message is also comes under TLS/DTLS   
3) If CER is received from any unknown peer then receiver should discard the message, or send the CEA with the Result-Code Avp set to DIAMETER\_UNKNOWN\_PEER.

If the local implementation policy permits to receive CER from unknown hosts, a successful CEA MAY be returned, and the life time of the peer entry in PEER-Table is equal to the lifetime of the transport connection. If in any case transport connection fails then all the pending transactions destined to the unknown peer can be discarded.  
  
The CER and CEA messages MUST NOT be proxied, redirected or relayed. Since CER/CEA messages cannot be proxied, but still it is possible that proxy will receive a CER message and proxy does not have any peer to handle the application requested in CER, in this case proxy set the E bit in CEA and set the Result-Code Avp to DIAMETER\_UNABLE\_TO\_DELIVER, sends back to CER generator peer.

For Example:- consider two nodes A and B and Node-A contains three applications X,Y,Z and two security mechanism s1 and s2 while Node-B contains two applications A,X and s1 security mechanism. Now Node-A will send CER to Node-B. Node -B will process the request and will create and send the CEA showing success and the common application i.e. X and s1 security mechanism. Now Node-A become aware of the fact that it can communicate for X application and s1 security mechanism.

Probable CER and CEA would be:-

      \_\_\_\_\_\_\_\_          CER                     \_\_\_\_\_\_\_\_

     | Node-A | ------------------------------>| Node-B |

     |\_\_\_\_\_\_\_\_| <------------------------------|\_\_\_\_\_\_\_\_|

                                          CEA

<CER> ::= < Diameter Header: 257, REQ >                          <CEA> ::= < Diameter Header: 257 >  
    { Origin-Host }                                               { Result-Code =SUCCESS}  
    { Origin-Realm }                                              { Origin-Host }

    {Host-IP-Address}                                            {Origin-Realm}  
    {Vendor-Id}                                                   {Host-IP-Address}    
    {Product-Name}                                                {Vendor-Id}   
    [Inband-Security-Id =s1]                                     {Product-Name}   
    [Inband-Security-Id =s2]                                      [Inband-Security-Id =s1]

    [Vendor-Specific-Application-Id =X]                          [Vendor-Specific-Application-Id =X]  
    [Vendor-Specific-Application-Id =Y]   
    [Vendor-Specific-Application-Id =Z]  

*CER/CEA Message Exchange*

**Gx Messages**

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

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

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

**CC-Request (CCR) Command**

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

Message Format:

<CC-Request> ::= < Diameter Header: 272, REQ, PXY >

< Session-Id >

{ Auth-Application-Id }

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ CC-Request-Type }

{ CC-Request-Number }

[ Destination-Host ]

[ Origin-State-Id ]

\*[ Subscription-Id ]

\*[ Supported-Features ]

[ Network-Request-Support ]

\*[ Packet-Filter-Information ]

[ Packet-Filter-Operation ]

[ Bearer-Identifier ]

[ Bearer-Operation ]

[ Framed-IP-Address ]

[ Framed-IPv6-Prefix ]

[ IP-CAN-Type ]

[ 3GPP-RAT-Type ]

[ RAT-Type ]

[ Termination-Cause ]

[ User-Equipment-Info ]

[ QoS-Information ]

[ QoS-Negotiation ]

[ QoS-Upgrade ]

[ Default-EPS-Bearer-QoS ]

0\*2[ AN-GW-Address ]

[ 3GPP-SGSN-MCC-MNC ]

[ 3GPP-SGSN-Address ]

[ 3GPP-SGSN-IPv6-Address ]

[ RAI ]

[ 3GPP-User-Location-Info]

[ 3GPP-MS-TimeZone ]

[ Called-Station-ID ]

[ PDN-Connection-ID ]

[ Bearer-Usage ]

[ Online ]

[ Offline ]

\*[ TFT-Packet-Filter-Information ]

\*[ Charging-Rule-Report]

\*[ Event-Trigger]

[ Event-Report-Indication]

[ Access-Network-Charging-Address ]

\*[ Access-Network-Charging-Identifier-Gx ]

\*[ CoA-Information ]

\*[ Usage-Monitoring-Information ]

[ Routing-Rule-Install ]

[ Routing-Rule-Remove ]

[ Maximum-Bandwidth ]

[ Logical-Access-ID ]

[ Physical-Access-ID ]

\*[ Proxy-Info ]

\*[ Route-Record ]

\*[ AVP ]

**CC-Answer (CCA) Command**

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

Message Format:

<CC-Answer> ::= < Diameter Header: 272, PXY >

< Session-Id >

{ Auth-Application-Id }

{ Origin-Host }

{ Origin-Realm }

[ Result-Code ]

[ Experimental-Result ]

{ CC-Request-Type }

{ CC-Request-Number }

\*[ Supported-Features ]

[ Bearer-Control-Mode ]

\*[ Event-Trigger ]

[ Origin-State-Id ]

\*[ Redirect-Host ]

[ Redirect-Host-Usage ]

[ Redirect-Max-Cache-Time ]

\*[ Charging-Rule-Remove ]

\*[ Charging-Rule-Install ]

[ Charging-Information ]

[ Online ]

[ Offline ]

\*[ QoS-Information ]

[ Revalidation-Time ]

[ Default-EPS-Bearer-QoS ]

[ Bearer-Usage ]

[ 3GPP-User-Location-Info]

\*[ Usage-Monitoring-Information ]

\*[ CSG-Information-Reporting ]

[ User-CSG-Information ]

[ Error-Message ]

[ Error-Reporting-Host ]

\*[ Failed-AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

\*[ AVP ]

**Re-Auth-Request (RAR) Command**

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PCRF to the PCEF in order to provision PCC rules using the PUSH procedure initiate the provision of unsolicited PCC rules. It is used to provision PCC rules, event triggers and event report indications for the session. If the PCRF performs the bearer binding, PCC rules will be provisioned at bearer level.

Message Format:

<RA-Request> ::= < Diameter Header: 258, REQ, PXY >

< Session-Id >

{ Auth-Application-Id }

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ Destination-Host }

{ Re-Auth-Request-Type }

[ Session-Release-Cause ]

[ Origin-State-Id ]

\*[ Event-Trigger ]

[ Event-Report-Indication ]

\*[ Charging-Rule-Remove ]

\*[ Charging-Rule-Install ]

[ Default-EPS-Bearer-QoS ]

\*[ QoS-Information ]

[ Revalidation-Time ]

\*[ Usage-Monitoring-Information ]

\*[ Proxy-Info ]

\*[ Route-Record ]

\*[ AVP]

**Re-Auth-Answer (RAA) Command**

The RAA command, indicated by the Command-Code field set to 258 and the 'R' bit cleared in the Command Flags field, is sent by the PCEF to the PCRF in response to the RAR command.

Message Format:

<RA-Answer> ::= < Diameter Header: 258, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

[ Result-Code ]

[ Experimental-Result ]

[ Origin-State-Id ]

[ IP-CAN-Type ]

[ RAT-Type ]

0\*2 [ AN-GW-Address ]

[ 3GPP-SGSN-MCC-MNC ]

[ 3GPP-SGSN-Address ]

[ 3GPP-SGSN-IPv6-Address ]

[ RAI ]

[ 3GPP-User-Location-Info ]

[ 3GPP-MS-TimeZone ]

\* [ Charging-Rule-Report]

[ Error-Message ]

[ Error-Reporting-Host ]

\* [ Failed-AVP ]

\* [ Proxy-Info ]

\* [ AVP ]

## 2.2.2 Rx messages

Existing Diameter command codes from the Diameter base protocol RFC 3588 [10] and the NASREQ Diameter application (RFC 4005 [12]) are used with the Rx specific AVPs. An Rx specific Auth‑Application id is used together with the command code to identify the Rx messages.

### **AA-Request (AAR) command**

The AAR command, indicated by the Command-Code field set to 265 and the 'R' bit set in the Command Flags field, is sent by an AF to the PCRF in order to provide it with the Session Information.

Message Format:

<AA-Request> ::= < Diameter Header: 265, REQ, PXY >

< Session-Id >

{ Auth-Application-Id }

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

[ Destination-Host ]

[ AF-Application-Identifier ]

\*[ Media-Component-Description ]

[ Service-Info-Status ]

[ AF-Charging-Identifier ]

[ SIP-Forking-Indication ]

\*[ Specific-Action ]

\*[ Subscription-Id ]

\*[ Supported-Features ]

[ Reservation-Priority ]

[ Framed-IP-Address ]

[ Framed-IPv6-Prefix ]

[ Called-Station-Id ]

[ Service-URN ]

[ Sponsored-Connectivity-Data ]

[ MPS-Identifier ]

[ Origin-State-Id ]

\*[ Proxy-Info ]

\*[ Route-Record ]

\*[ AVP ]

### 

### **AA-Answer (AAA) command**

### The AAA command, indicated by the Command-Code field set to 265 and the 'R' bit cleared in the Command Flags field, is sent by the PCRF to the AF in response to the AAR command.

Message Format:

<AA-Answer> ::= < Diameter Header: 265, PXY >

< Session-Id >

{ Auth-Application-Id }

{ Origin-Host }

{ Origin-Realm }

[ Result-Code ]

[ Experimental-Result ]

\*[ Access-Network-Charging-Identifier ]

[ Access-Network-Charging-Address ]

[ Acceptable-Service-Info ]

[ IP-CAN-Type ]

[ RAT-Type ]

\*[ Flows ]

\*[ Supported-Features ]

\*[ Class ]

[ Error-Message ]

[ Error-Reporting-Host ]

\*[ Failed-AVP ]

[ Origin-State-Id ]

\*[ Redirect-Host ]

[ Redirect-Host-Usage ]

[ Redirect-Max-Cache-Time ]

\*[ Proxy-Info ]

\*[ AVP ]

### **Re-Auth-Request (RAR) command**

The RAR command, indicated by the Command-Code field set to 258 and the 'R' bit set in the Command Flags field, is sent by the PCRF to the AF in order to indicate an Rx specific action.

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 ]

[ Sponsored-Connectivity-Data ]

[ Origin-State-Id ]

\*[ Class ]

\*[ Proxy-Info ]

\*[ Route-Record ]

\*[ AVP ]

### **Re-Auth-Answer (RAA) command**

The RAA command, indicated by the Command-Code field set to 258 and the 'R' bit cleared in the Command Flags field, is sent by the AF to the PCRF in response to the RAR command.

Message Format:

<RA-Answer> ::= < Diameter Header: 258, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

[ Result-Code ]

[ Experimental-Result ]

\*[ Media-Component-Description ]

[ Service-URN ]

[ Origin-State-Id ]

\*[ Class ]

[ Error-Message ]

[ Error-Reporting-Host ]

\*[ Redirect-Host ]

[ Redirect-Host-Usage ]

[ Redirect-Max-Cache-Time ]

\*[ Failed-AVP ]

\*[ Proxy-Info ]

\*[ AVP ]

### **Session-Termination-Request (STR) command**

The STR command, indicated by the Command-Code field set to 275 and the 'R' bit set in the Command Flags field, is sent by the AF to inform the PCRF that an established session shall be terminated.

Message Format:

<ST-Request> ::= < Diameter Header: 275, REQ, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ Auth-Application-Id }

{ Termination-Cause }

[ Destination-Host ]

\*[ Class ]

[ Origin-State-Id ]

\*[ Proxy-Info ]

\*[ Route-Record ]

\*[ AVP ]

### **Session-Termination-Answer (STA) command**

The STA command, indicated by the Command-Code field set to 275 and the 'R' bit cleared in the Command Flags field, is sent by the PCRF to the AF in response to the STR command.

Message Format:

<ST-Answer> ::= < Diameter Header: 275, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

[ Result-Code ]

[ Error-Message ]

[ Error-Reporting-Host ]

\* [ Failed-AVP ]

**[ Sponsored-Connectivity-Data ]**

[ Origin-State-Id ]

\*[ Class ]

\*[ Redirect-Host ]

[ Redirect-Host-Usage ]

[ Redirect-Max-Cache-Time ]

\*[ Proxy-Info ]

\*[ AVP ]

### **Abort-Session-Request (ASR) command**

The ASR command, indicated by the Command-Code field set to 274 and the 'R' bit set in the Command Flags field, is sent by the PCRF to inform the AF that bearer for the established session is no longer available.

Message Format:

<AS-Request> ::= < Diameter Header: 274, REQ, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

{ Destination-Realm }

{ Destination-Host }

{ Auth-Application-Id }

**{ Abort-Cause }**

[ Origin-State-Id ]

\*[ Proxy-Info ]

\*[ Route-Record ]

\*[ AVP ]

### **Abort-Session-Answer (ASA) command**

The ASA command, indicated by the Command-Code field set to 274 and the 'R' bit cleared in the Command Flags field, is sent by the AF to the PCRF in response to the ASR command.

Message Format:

<AS-Answer> ::= < Diameter Header: 274, PXY >

< Session-Id >

{ Origin-Host }

{ Origin-Realm }

[ Result-Code ]

[ Origin-State-Id ]

[ Error-Message ]

[ Error-Reporting-Host ]

\*[ Failed-AVP ]

\*[ Redirect-Host ]

[ Redirect-Host-Usage ]

[ Redirect-Max-Cache-Time ]

\*[ Proxy-Info ]

\*[ AVP ]

# 2.2.3 Diameter application for Sh interface

This clause specifies a Diameter application that allows a Diameter server and a Diameter client:

- to download and update transparent and non-transparent user data

- to request and send notifications on changes on user data

The Sh interface protocol is defined as an IETF vendor specific Diameter application, where the vendor is 3GPP. The vendor identifier assigned by IANA to 3GPP ( [http://www.iana.org/assignments/enterprise-numbers](http://www.isi.edu/in-notes/iana/assignments/enterprise-numbers)) is 10415.

The Diameter application identifier assigned to the Sh interface application is 16777217 (allocated by IANA).

### **User-Data-Request (UDR) Command**

The User-Data-Request (UDR) command, indicated by the Command-Code field set to 306 and the ‘R’ bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request user data.

Message Format

< User-Data -Request> ::= < Diameter Header: 306, REQ, PXY, 16777217 >

< Session-Id >

{ Vendor-Specific-Application-Id }

{ Auth-Session-State }

{ Origin-Host }

{ Origin-Realm }

[ Destination-Host ]

{ Destination-Realm }

\*[ Supported-Features ]

{ User-Identity }

[ Wildcarded-PSI ]

[ Wildcarded-IMPU ]

[ Server-Name ]

\*[ Service-Indication ]

\*{ Data-Reference }

\*[ Identity-Set ]

[ Requested-Domain ]

[ Current-Location ]

\*[ DSAI-Tag ]

[ Session-Priority ]

[ User-Name ]

[ Requested-Nodes ]

[ Serving-Node-Indication ]

\*[ AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

### **User-Data-Answer (UDA) Command**

The User-Data-Answer (UDA) command, indicated by the Command-Code field set to 306 and the ‘R’ bit cleared in the Command Flags field, is sent by a server in response to the User-Data-Request command. The Experimental-Result AVP may contain one of the values defined in section 6.2 or in 3GPP TS 29.229 [6].

Message Format

< User-Data-Answer > ::= < Diameter Header: 306, PXY, 16777217 >

< Session-Id >

{ Vendor-Specific-Application-Id }

[ Result-Code ]

[ Experimental-Result ]

{ Auth-Session-State }

{ Origin-Host }

{ Origin-Realm }

\*[ Supported-Features ]

[ Wildcarded-PSI ]

[ Wildcarded-IMPU ]

[ User-Data ]

\*[ AVP ]

\*[ Failed-AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

### **Profile-Update-Request (PUR) Command**

The Profile-Update-Request (PUR) command, indicated by the Command-Code field set to 307 and the ‘R’ bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to update user data in the server.

Message Format

< Profile-Update-Request > ::= < Diameter Header: 307, REQ, PXY, 16777217 >

< Session-Id >

{ Vendor-Specific-Application-Id }

{ Auth-Session-State }

{ Origin-Host }

{ Origin-Realm }

[ Destination-Host ]

{ Destination-Realm }

**\*[ Supported-Features ]**

**{ User-Identity }**

**[ Wildcarded-PSI ]**

**[ Wildcarded-IMPU ]**

[ User-Name ]

**{** Data-Reference **}**

{ User-Data }

\*[ AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

### **Profile-Update-Answer (PUA) Command**

The Profile-Update-Answer (PUA) command, indicated by the Command-Code field set to 307 and the ‘R’ bit cleared in the Command Flags field, is sent by a server in response to the Profile-Update-Request command. The Experimental-Result AVP may contain one of the values defined in section 6.2 or in 3GPP TS 29.229 [6].

Message Format

< Profile-Update-Answer > ::=< Diameter Header: 307, PXY, 16777217 >

< Session-Id >

{ Vendor-Specific-Application-Id }

[ Result-Code ]

[ Experimental-Result ]

{ Auth-Session-State }

{ Origin-Host }

{ Origin-Realm }

**[ Wildcarded-PSI ]**

**[ Wildcarded-IMPU ]**

\*[ Supported-Features ]

\*[ AVP ]

\*[ Failed-AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

### **Subscribe-Notifications-Request (SNR) Command**

The Subscribe-Notifications-Request (SNR) command, indicated by the Command-Code field set to 308 and the ‘R’ bit set in the Command Flags field, is sent by a Diameter client to a Diameter server in order to request notifications of changes in user data.

Message Format

< Subscribe-Notifications-Request > ::=< Diameter Header: 308, REQ, PXY, 16777217 >

< Session-Id >

{ Vendor-Specific-Application-Id }

{ Auth-Session-State }

{ Origin-Host }

{ Origin-Realm }

[ Destination-Host ]

{ Destination-Realm }

\*[ Supported-Features ]

{ User-Identity }

[ Wildcarded-PSI ]

[ Wildcarded-IMPU ]

\*[ Service-Indication ]

[ Send-Data-Indication ]

[ Server-Name ]

{ Subs-Req-Type }

\*{ Data-Reference }

\*[ Identity-Set ]

[ Expiry-Time ]

\*[ DSAI-Tag ]

[One-Time-Notification]

[ User-Name ]

\*[ AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

### **Subscribe-Notifications-Answer (SNA) Command**

The Subscribe-Notifications-Answer command, indicated by the Command-Code field set to 308 and the ‘R’ bit cleared in the Command Flags field, is sent by a server in response to the Subscribe-Notifications-Request command. The Result-Code or Experimental-Result AVP may contain one of the values defined in section 6.2 or in 3GPP TS 29.229 [6].

Message Format

< Subscribe-Notifications-Answer > ::=< Diameter Header: 308, PXY, 16777217 >

< Session-Id >

{ Vendor-Specific-Application-Id }

{ Auth-Session-State }

[ Result-Code ]

[ Experimental-Result ]

{ Origin-Host }

{ Origin-Realm }

**[ Wildcarded-PSI ]**

**[ Wildcarded-IMPU ]**

**\*[ Supported-Features ]**

**[ User-Data ]**

**[ Expiry-Time ]**

\*[ AVP ]

\*[ Failed-AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

### **Push-Notification-Request (PNR) Command**

The Push-Notification-Request (PNR) command, indicated by the Command-Code field set to 309 and the ‘R’ bit set in the Command Flags field, is sent by a Diameter server to a Diameter client in order to notify changes in the user data in the server.

Message Format

< Push-Notification-Request > ::=< Diameter Header: 309, REQ, PXY, 16777217 >

< Session-Id >

{ Vendor-Specific-Application-Id }

{ Auth-Session-State }

{ Origin-Host }

{ Origin-Realm }

{ Destination-Host }

{ Destination-Realm }

\*[ Supported-Features ]

{ User-Identity }

[ Wildcarded-PSI ]

[ Wildcarded-IMPU ]

[ User-Name ]

{ User-Data }

\*[ AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

### **Push-Notifications-Answer (PNA) Command**

The Push-Notifications-Answer (PNA) command, indicated by the Command-Code field set to 309 and the ‘R’ bit cleared in the Command Flags field, is sent by a client in response to the Push-Notification-Request command. The Experimental-Result AVP may contain one of the values defined in section 6.2 or in 3GPP TS 29.229 [6].

Message Format

< Push-Notification-Answer > ::=< Diameter Header: 309, PXY, 16777217 >

< Session-Id >

{ Vendor-Specific-Application-Id }

[ Result-Code ]

[ Experimental-Result ]

{ Auth-Session-State }

{ Origin-Host }

{ Origin-Realm }

\*[ Supported-Features ]

\*[ AVP ]

\*[ Failed-AVP ]

\*[ Proxy-Info ]

\*[ Route-Record ]

**Chapter 3**

**Result Codes**

## **Result-Code AVP values**

This section defines new result code values that must be supported by all Diameter implementations that conform to this specification. The result codes defined in 3GPP TS 29.229 [6] are also applicable. When one of the result codes defined here is included in a response, it shall be inside an Experimental-Result AVP and Result-Code AVP shall be absent.

### **Success**

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

No result codes within this category have been defined so far.

### **Permanent Failures**

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

#### DIAMETER\_ERROR\_USER\_DATA\_NOT\_RECOGNIZED (5100)

The data received by the AS is not supported or recognized.

#### DIAMETER\_ERROR\_OPERATION\_NOT\_ALLOWED (5101)

The requested operation is not allowed for the user

#### DIAMETER\_ERROR\_USER\_DATA\_CANNOT\_BE\_READ (5102)

The requested user data is not allowed to be read.

#### DIAMETER\_ERROR\_USER\_DATA\_CANNOT\_BE\_MODIFIED (5103)

The requested user data is not allowed to be modified.

#### DIAMETER\_ERROR\_USER\_DATA\_CANNOT\_BE\_NOTIFIED (5104)

The requested user data is not allowed to be notified on changes.

#### DIAMETER\_ERROR\_TOO\_MUCH\_DATA (5008)

The size of the data pushed to the receiving entity exceeds its capacity. This error code is defined in 3GPP TS 29.229 [6].

#### DIAMETER\_ERROR\_TRANSPARENT\_DATA OUT\_OF\_SYNC (5105)

The request to update the repository data at the HSS could not be completed because the requested update is based on an out-of-date version of the repository data. That is, the sequence number in the Sh-Update Request message, does not match with the immediate successor of the associated sequence number stored for that repository data at the HSS. It is also used where an AS tries to create a new set of repository data when the identified repository data already exists in the HSS.

#### DIAMETER\_ERROR\_SUBS\_DATA\_ABSENT (5106)

The Application Server requested to subscribe to changes to Repository Data that is not present in the HSS.

#### DIAMETER\_ERROR\_NO\_SUBSCRIPTION\_TO\_DATA (5107)

The AS received a notification of changes of some information to which it is not subscribed.

#### DIAMETER\_ERROR\_DSAI\_NOT\_AVAILABLE (5108)

The Application Server addressed a DSAI not configured in the HSS.

### 

### **Transient Failures**

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

#### DIAMETER\_USER\_DATA\_NOT\_AVAILABLE (4100)

The requested user data is not available at this time to satisfy the requested operation.

#### DIAMETER\_PRIOR\_UPDATE\_IN\_PROGRESS (4101)

The request to update the repository data at the HSS could not be completed because the related repository data is currently being updated by another entity.

**Conclusion**

Thus the project on Policy and Charging Rules Functions has successfully been worked on. The various messages on the different interfaces namely Sh, Rx and Gx have been worked on and explored.

The role of PCRF has been understood as 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.

**References**

[1] 3GPP TS 29.329 V10.2.0 (2011-03) *Technical Specification* 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals ; Sh Interface based on the Diameter protocol; Protocol details (Release 10).

[2] 3GPP TS 29.212 V10.4.0 (2011-09) *Technical Specification* 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control (PCC) over Gx reference point (Release 10).

[3] 3GPP TS 29.214 V10.13.0 (2014-03) Technical Specification 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Policy and Charging Control over Rx reference point (Release 10).

[4] RFC 6733 Diameter Base Protocol *PROPOSED STANDARD*. Standards Track. ISSN 2070-1721