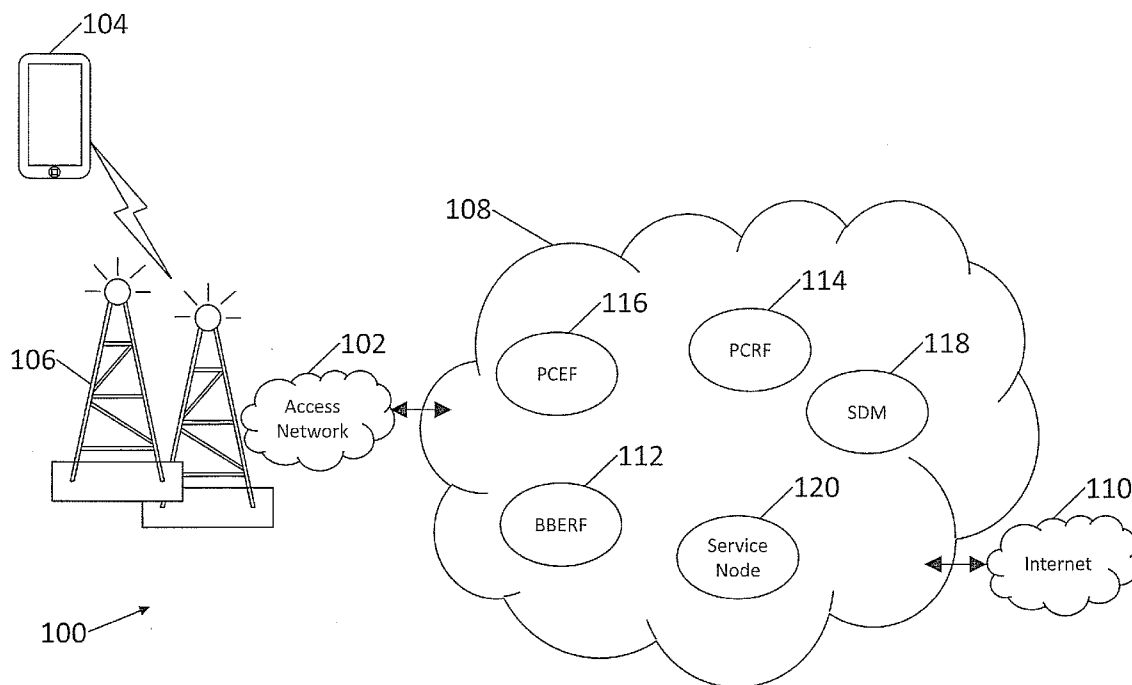




US 20110225280A1

(19) **United States**(12) **Patent Application Publication**
DELSESTO et al.(10) **Pub. No.: US 2011/0225280 A1**(43) **Pub. Date: Sep. 15, 2011**(54) **METHODS, SYSTEMS, AND COMPUTER
READABLE MEDIA FOR COMMUNICATING
POLICY INFORMATION BETWEEN A
POLICY CHARGING AND RULES FUNCTION
AND A SERVICE NODE****Publication Classification**(51) **Int. Cl.**
G06F 15/173 (2006.01)(52) **U.S. Cl.** **709/223**(76) **Inventors:** **Mark DELSESTO**, Hudson, NH
(US); **Michael Mercurio**, Jamaica
Plan, MA (US); **Tarek**
Abou-Assali, Boston, MA (US);
Uri Baniel, Buffalo Grove, IL (US)(21) **Appl. No.: 13/048,607**(22) **Filed: Mar. 15, 2011****Related U.S. Application Data**(60) Provisional application No. 61/313,953, filed on Mar.
15, 2010, provisional application No. 61/315,130,
filed on Mar. 18, 2010, provisional application No.
61/322,533, filed on Apr. 9, 2010.(57) **ABSTRACT**

According to one aspect, the subject matter described herein includes a method for communicating policy information. The method includes steps occurring at a policy charging and rules function (PCRF) node. The method also includes receiving, from a service node, a message requesting a policy rule, wherein the message includes an Internet protocol (IP) address associated with a subscriber. The method further includes determining a network access identifier (NAI) for the subscriber based on the IP address. The method further includes selecting a policy rule for the subscriber based on the NAI. The method further includes communicating the policy rule to the service node.



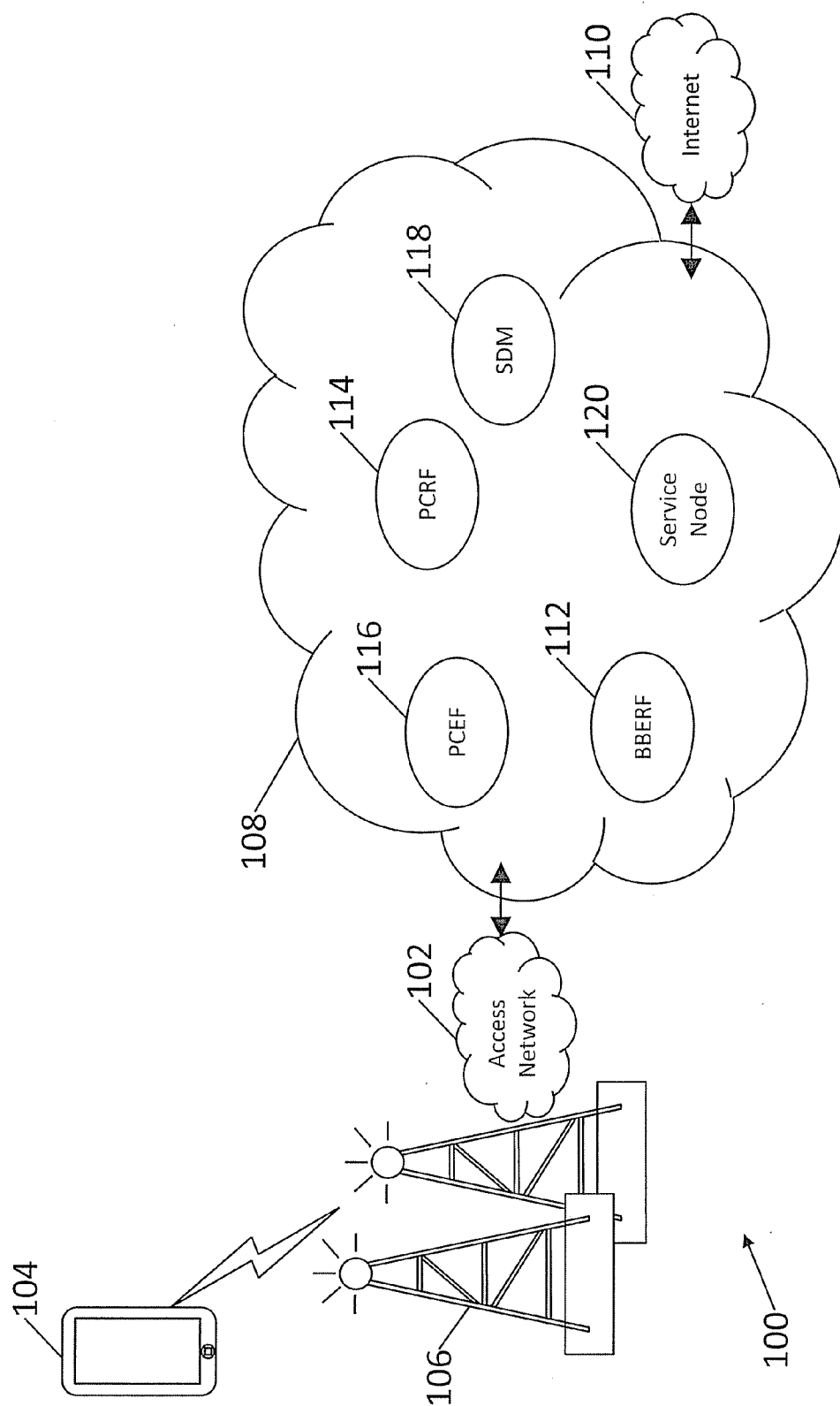


FIG. 1

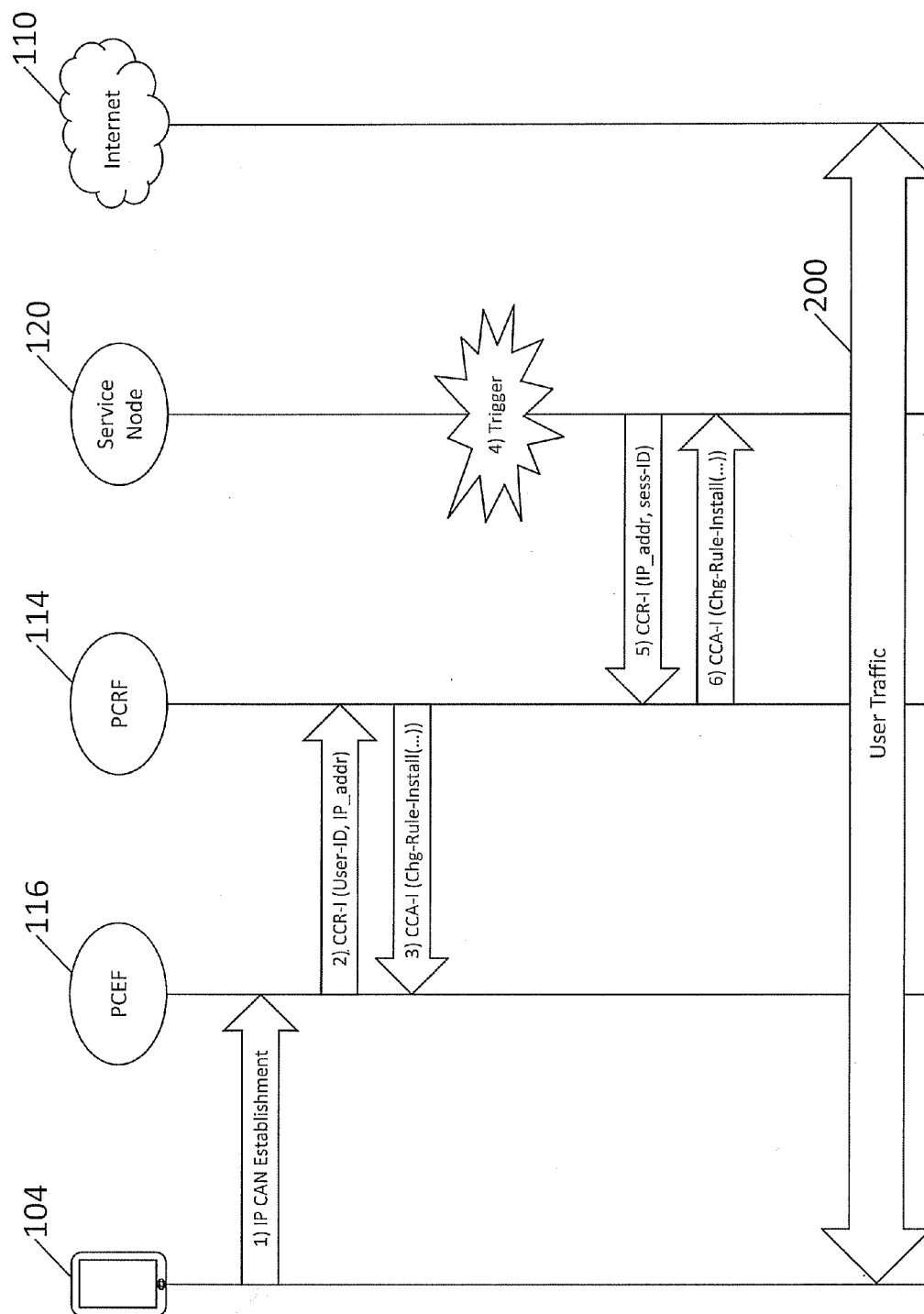


FIG. 2

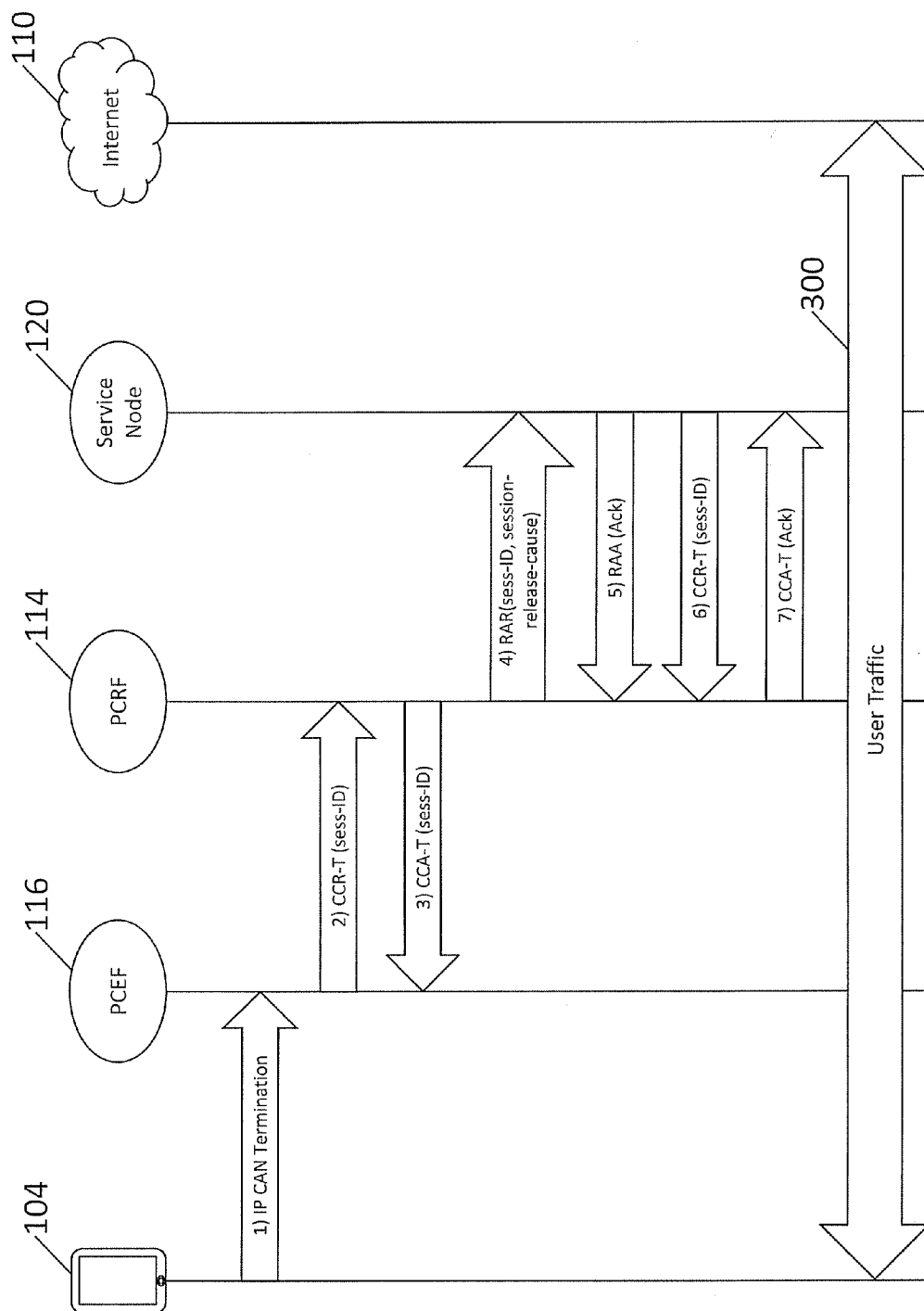


FIG. 3

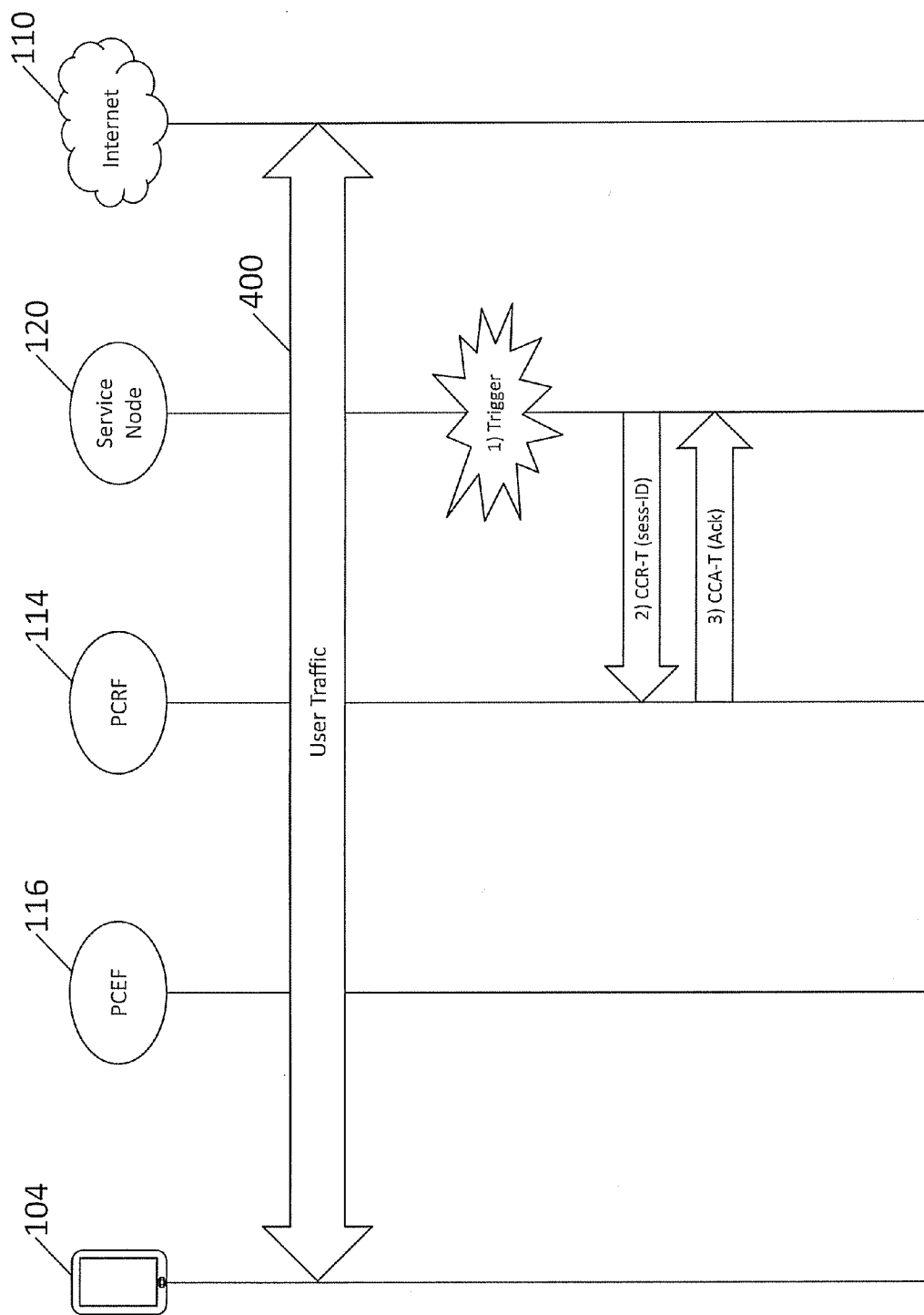


FIG. 4

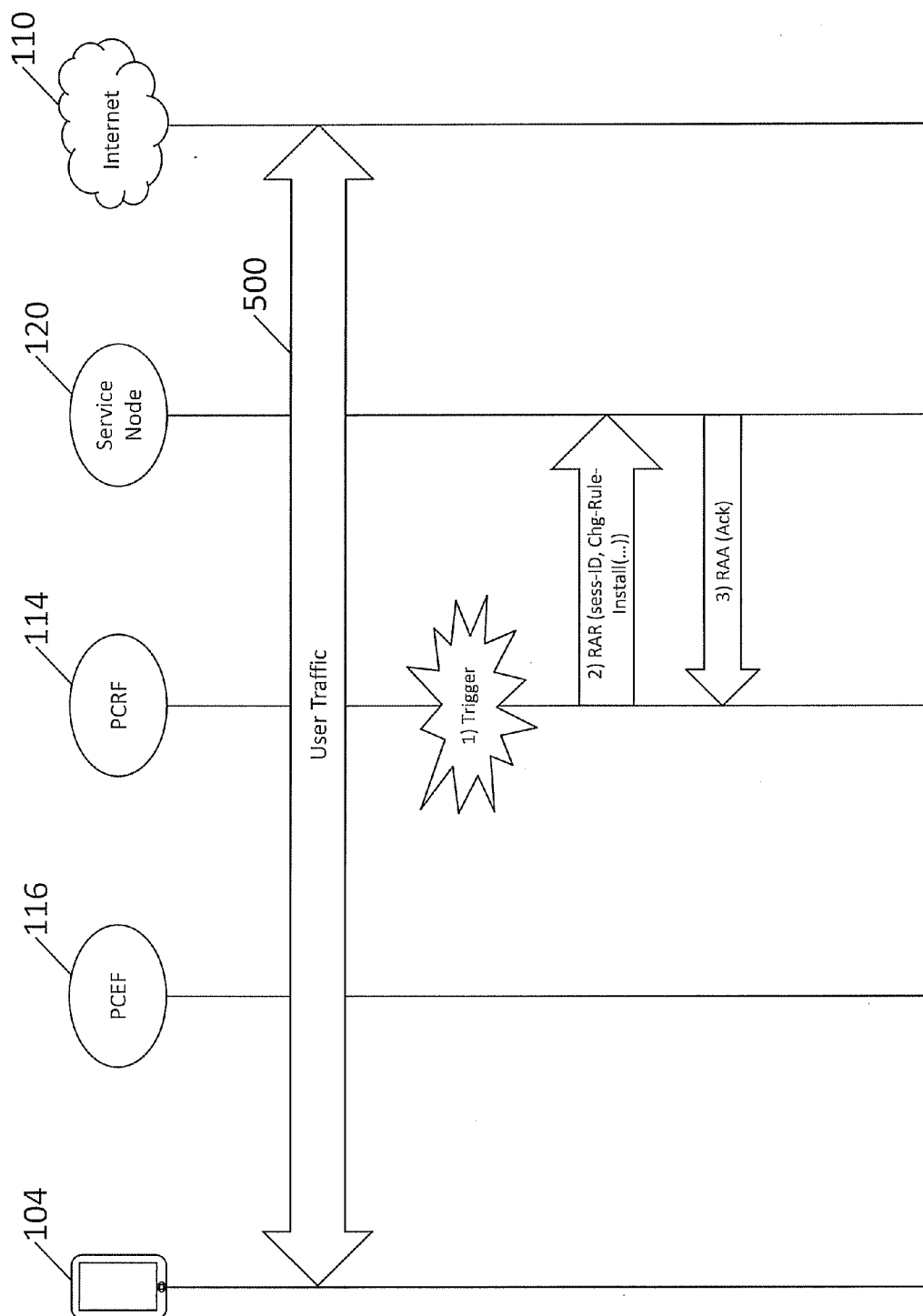


FIG. 5

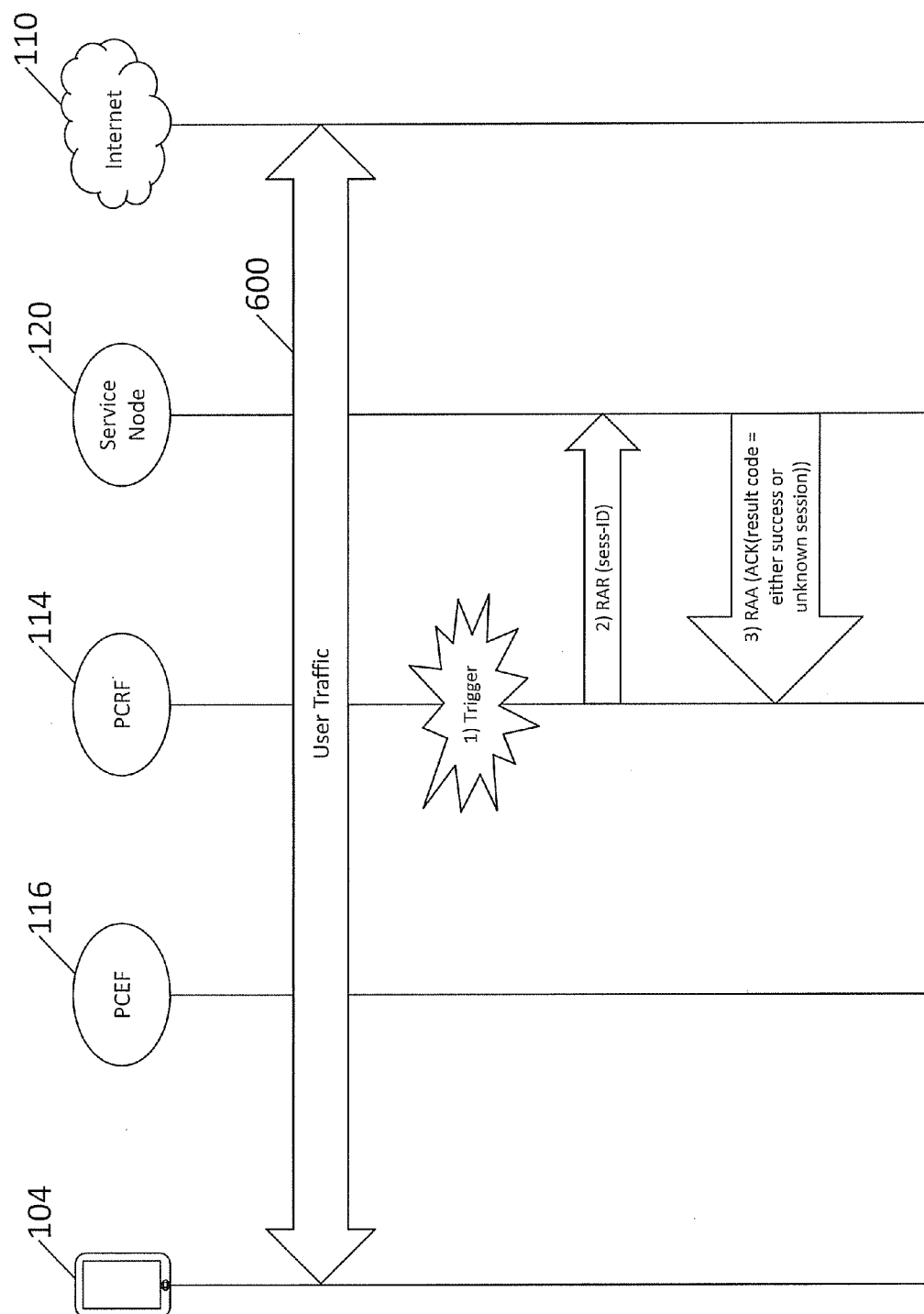


FIG. 6

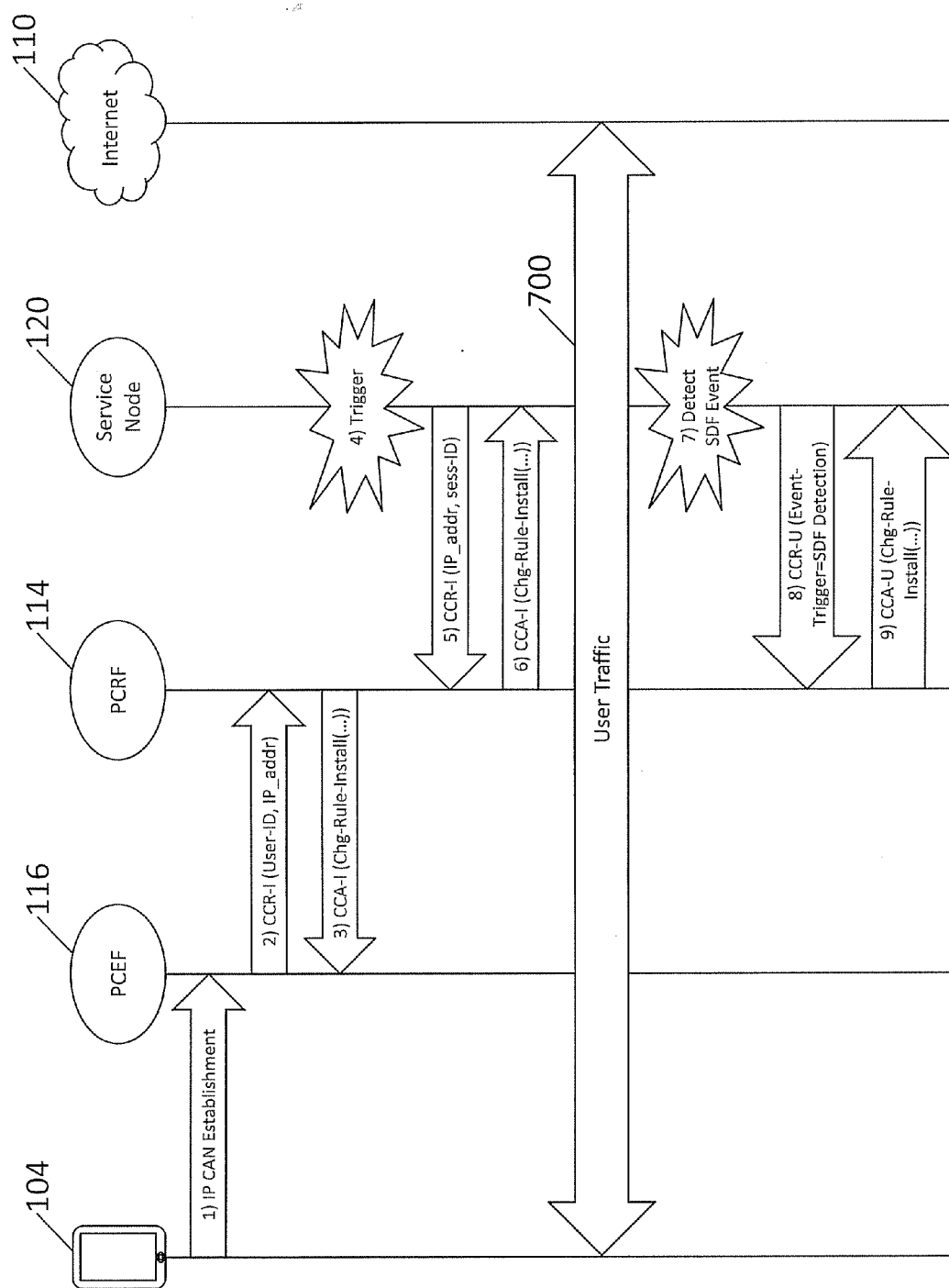


FIG. 7

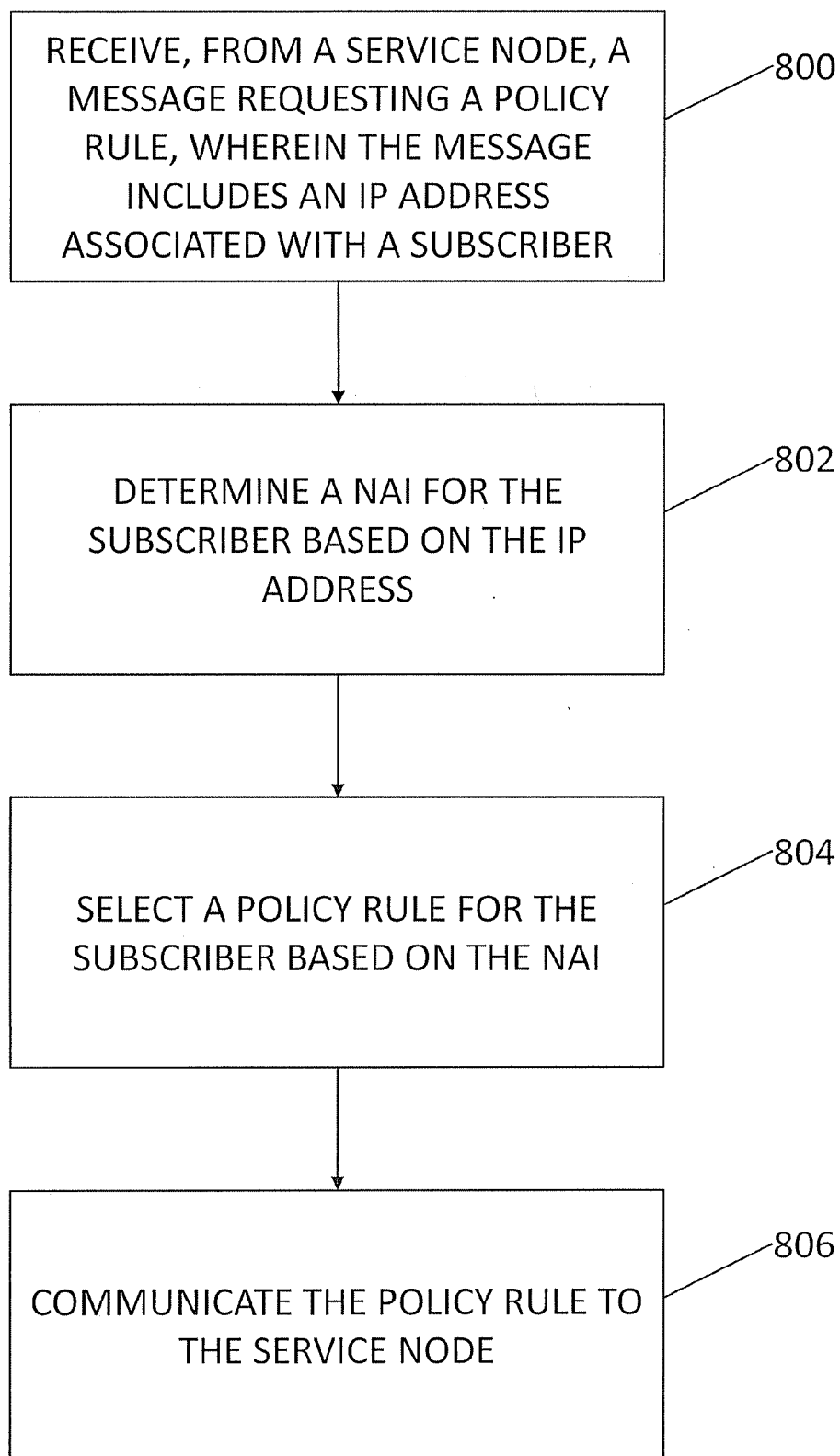


FIG. 8

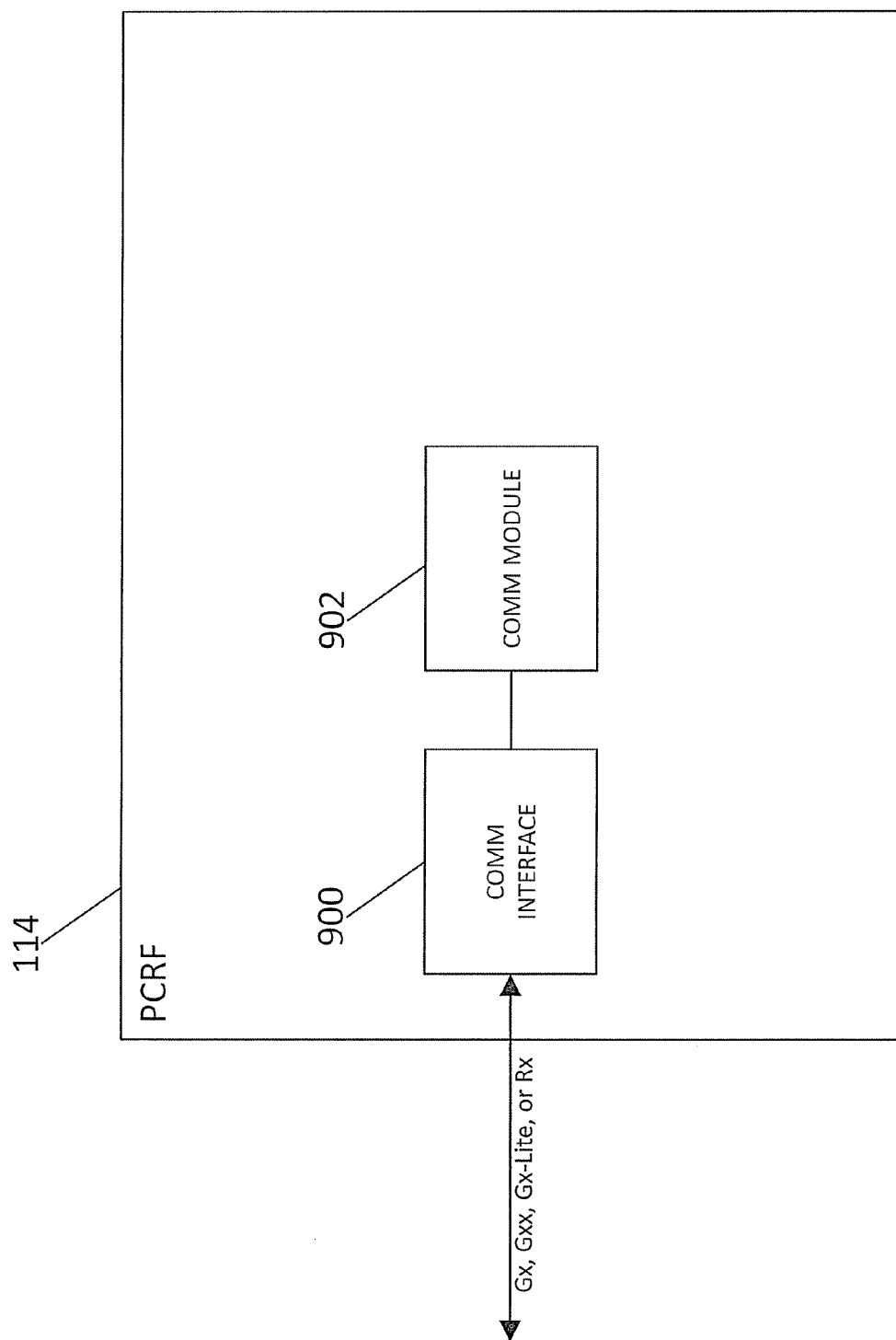


FIG. 9

**METHODS, SYSTEMS, AND COMPUTER
READABLE MEDIA FOR COMMUNICATING
POLICY INFORMATION BETWEEN A
POLICY CHARGING AND RULES FUNCTION
AND A SERVICE NODE**

PRIORITY CLAIM

[0001] This application claims the benefit of U.S. Provisional Patent Application Ser. No. 61/313,953, filed Mar. 15, 2010; U.S. Provisional Patent Application Ser. No. 61/315,130, filed Mar. 18, 2010; and U.S. Provisional Patent Application Ser. No. 61/322,533, filed Apr. 9, 2010; the disclosure of which are incorporated herein by reference in their entirety.

TECHNICAL FIELD

[0002] The subject matter described herein relates to communicating policy information between a policy charging and rules function and a service node. More specifically, the subject matter relates to methods, systems, and computer readable media for communicating policy information between a policy charging and rules function and a service node.

BACKGROUND

[0003] A policy charging and rules function (PCRF) node may be utilized by multimedia networks to determine policy rules in real-time. Utilization of a PCRF may aid a network operator in making real-time, subscriber specific, policy decisions that may be utilized to provide varying levels of quality of service (QoS).

[0004] Telecommunications networks may include various service nodes for performing a variety of services. Service nodes may include functionality for deep packet inspection (DPI), content-filtering, and/or web-optimization. DPI is the use of a packet's non-header information by a network entity that is not an endpoint for that packet. DPI is employed by network operators for a wide variety of uses, e.g., anti-virus, spam filtering, intrusion detection, and gathering statistical information. Content-filtering is the blocking of specified content based on analysis of the content itself rather than other criteria such as its source. Web-optimization is provided to enhance a user's experience and may involve refining and/or altering content to better suit the hardware and/or software utilized by a particular user.

[0005] Based on operator policy, a PCRF node may need to communicate policy information between itself and a service node.

[0006] Accordingly, a need exists for methods, systems, and computer readable media for communicating policy information between a policy charging and rules function and a service node.

SUMMARY

[0007] According to one aspect, the subject matter described herein includes a method for communicating policy information. The method includes steps occurring at a policy charging and rules function (PCRF) node. The method also includes receiving, from a service node, a message requesting a policy rule, wherein the message includes an Internet protocol (IP) address associated with a subscriber. The method further includes determining a network access identifier (NAI) for the subscriber based on the IP address. The method further includes selecting a policy rule for the

subscriber based on the NAI. The method further includes communicating the policy rule to the service node.

[0008] According to another aspect, the subject matter described herein includes a system for communicating policy information. The system includes a PCRF node. The PCRF node includes a communication interface. The PCRF node further includes a communication module. The communication module is configured to utilize the communication interface to receive, from a service node, a message requesting a policy rule, wherein the message includes an IP address associated with a subscriber. The communication module is further configured to determine a NAI for the subscriber based on the IP address. The communication module is further configured to select a policy rule for the subscriber based on the NAI. The communication module is further configured to utilize the communication interface to communicate the policy rule to the service node.

[0009] As used herein, the term "node" refers to a physical computing platform including one or more processors and memory.

[0010] The subject matter described herein can be implemented in software in combination with hardware and/or firmware. For example, the subject matter described herein may be implemented in software executed by one or more processors. In one exemplary implementation, the subject matter described herein may be implemented using a non-transitory computer readable medium having stored thereon computer executable instructions that when executed by the processor of a computer control the computer to perform steps. Exemplary computer readable media suitable for implementing the subject matter described herein include non-transitory computer readable media, such as disk memory devices, chip memory devices, programmable logic devices, and application specific integrated circuits. In addition, a computer readable medium that implements the subject matter described herein may be located on a single device or computing platform or may be distributed across multiple devices or computing platforms.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] The subject matter described herein will now be explained with reference to the accompanying drawings of which:

[0012] FIG. 1 is a network diagram illustrating an exemplary network environment for communicating policy information according to an embodiment of the subject matter described herein;

[0013] FIG. 2 is a message flow diagram illustrating the communication of policy information in response to an external trigger according to an embodiment of the subject matter described herein;

[0014] FIG. 3 is a message flow diagram illustrating an exemplary PCRF initiated termination of a session for communicating policy information according to an embodiment of the subject matter described herein;

[0015] FIG. 4 is a message flow diagram illustrating an exemplary externally initiated termination of a session for communicating policy information according to an embodiment of the subject matter described herein;

[0016] FIG. 5 is a message flow diagram illustrating an exemplary policy rule push for communicating policy information according to an embodiment of the subject matter described herein;

[0017] FIG. 6 is a message flow diagram illustrating an exemplary audit procedure for communicating policy information according to an embodiment of the subject matter described herein;

[0018] FIG. 7 is a message flow diagram illustrating exemplary event subscription and notification for communicating policy information according to an embodiment of the subject matter described herein;

[0019] FIG. 8 is a flow chart illustrating an exemplary process for communicating policy information according to an embodiment of the subject matter described herein; and

[0020] FIG. 9 is a block diagram of an exemplary PCRF node for communicating policy information according to an embodiment of the subject matter described herein.

DETAILED DESCRIPTION

[0021] Methods, systems, and computer readable media for communicating policy information are provided. FIG. 1 is a network diagram illustrating an exemplary network environment for communicating policy information according to an embodiment of the subject matter described herein. Referring to FIG. 1, network environment 100 may include access network 102. Access network 102 may include nodes, functions, devices, and/or components for providing user equipment (UE) 104 access to services, functions, or devices in one or more networks. In one embodiment, access network 102 may be a radio access network (RAN). For example, access network 102 may be a global system for mobile communications (GSM) RAN (GRAN), a general packet radio service (GPRS) access network, a universal mobile telecommunications system (UMTS) RAN (UTRAN), an evolved UTRAN (eUTRAN), an Internet protocol (IP) connectivity access network (IPCAN), a code division multiple access (CDMA) network, an evolution-data optimized (EV-DO) network, a wideband CDMA (WCDMA) network, a high speed packet access (HSPA) network, an evolved HSPA (EHSPA+) network, or a long term evolution (LTE) access network. Access network 102 may include one or more transceiver nodes 106 for communicating with UE 104. UE 104 may include a computer, a pager, a mobile phone, a smartphone, a wireless modem, or other devices through which a subscriber accesses network services.

[0022] Network environment 100 may further include a carrier network 108. Carrier network 108 may be utilized by UE 104 to access Internet 110. Carrier network 108 may include a bearer binding and event reporting function (BBERF) node 112. BBERF node 112 may be, for example, a service gateway (SGW) or a serving general packet radio service (GPRS) support node (SGSN). Carrier network 108 may further include a PCRF node 114. PCRF node 114 is a centralized node that can act as a policy decision point for carrier network 108. PCRF node 114 may take operator defined service policies, subscription information pertaining to a user, and other data into account to build policy decisions. Policy decisions may be formulated as policy control and charging (PCC) rules. PCC rules may contain information about user plane traffic expressed as a packet filter. A packet filter may take the form of an IP five-tuple specifying: (1) source IP address(es), (2) destination IP address(es), (3) source port number(s), (4) destination port number(s), and (5) application protocol(s) (e.g., transmission control protocol (TCP), user datagram protocol (UDP)). All IP packets matching a packet filter of a PCC rule may be designated an SDF.

[0023] Flow-based charging models may introduce the ability to charge for SDFs identified by service data flow filters according to specified charging rules. Charging rules may contain information that allows the filtering of traffic to identify packets belonging to a particular SDF (e.g., IP multimedia subsystem (IMS), file transfer protocol (FTP), browsing) and allow an operator to define how a particular SDF is to be charged (e.g., different media streams within a single packet data protocol (PDP) context.) Charging rules may be requested by a policy and charging enforcement function (PCEF) node (e.g., by a packet data network (PDN) gateway in an evolved packet system (EPS)), at bearer establishment, upon a specified trigger event, and/or upon bearer termination. Such a request may be made using a Gx reference point towards a PCRF.

[0024] Carrier network 108 may also include PCEF node 116. PCEF node 116 may serve as a policy enforcement point and may be placed in line between access network 102 and PCRF node 114. PCEF node 116 may be, for example, a gateway GPRS support node (GGSN) or a PDN gateway. As an enforcement point, PCEF node 116 may request and receive policy rules from PCRF node 114. Policy rules may take the form of, for example, Gx rules contained in credit control messages.

[0025] Carrier network 108 may also include subscriber data management (SDM) node 118. SDM node 118 may contain a comprehensive subscriber database, including information pertaining to subscribers' locations and Internet protocol information. SDM node 118 may be, for example, a home subscriber server (HSS), a subscription profile repository (SPR), or a user profile serving function (UPSF).

[0026] Carrier network 108 may further include service node 120. Service node 120 may include functionality for DPI, content-filtering, and/or web-optimization. DPI is the use of a packet's non-header information by a network entity that is not an endpoint for that packet. For example, service node 120 may include functionality enabling it to examine packets originating in Internet 110 and destined for UE 104. Content-filtering is the blocking of specified content based on analysis of the content itself rather than other criteria such as its source. For example, service node 120 may include functionality enabling it to analyze the content of packets originating in Internet 110 and destined for UE 104. Based on such content-analysis, service node 120 may filter or prevent the content from reaching UE 104. Web-optimization is provided to enhance a user's experience and may involve refining and/or altering content to better suit the hardware and/or software utilized by a particular user. For example, service node 120 may include functionality enabling it to optimize content originating in Internet 110 and destined for UE 104 based on, for example, the type of device UE 104 is. For example, service node 120 may detect video streaming from a source located in Internet 110 and destined for UE 104. In response, service node 120 may, for example, resize the video for optimal display on UE 104. A service node may or may not support the full blown Gx protocol as specified in 3GPP 29.212. For example, service node 120 may not include support for the full blown Gx protocol. In accordance with embodiments of the subject matter described herein, a service node that does not include support for the full blown Gx protocol may communicate with a PCRF node, enabling it to subscribe to SDF event notifications and install policy rules.

[0027] FIG. 2 is a message flow diagram illustrating the communication of policy information in response to an exter-

nal trigger according to an embodiment of the subject matter described herein. Referring to FIG. 2, at step 1, UE 104 may initiate establishment of an IP CAN session with PCEF node 116 for the purpose of communicating with a host in Internet 110. At step 2, PCEF node 116 may send a credit-control-request initial (CCR-I) message to PCRF node 114. The CCR-I message may include a user ID and IP address associated with UE 104. At step 3, PCRF node 114 may send a credit-control-answer initial (CCA-I) message to PCEF node 116. The CCA-I message may include a charging rule for PCEF node 116 to implement with respect to UE 104's IP CAN session. PCEF node 116 may support an implementation of the full blown Gx protocol and thus the CCR-I/CCA-I exchange, between PCEF node 116 and PCRF node 114, may utilize the Gx protocol.

[0028] User data plane 200, carrying traffic associated with UE 104's IP CAN session, may traverse service node 120. PCRF node 114 may desire to communicate with service node 120 in order to subscribe to SDF event notifications and/or install policy rule(s). Service node 120 may not implement the full blown Gx protocol and thus utilization of the Gx protocol may not be possible. In accordance with embodiments of the subject matter described herein, PCRF node 114 and service node 120 may utilize a subset of the Gx application/protocol that does not include all of the parameter/attribute value pairs (AVPs) designated as mandatory in 3GPP 29.212 to communicate (hereinafter "Gx-Lite"). At step 4, service node 120 may receive an external trigger. For example, commonly owned, co-pending U.S. patent application entitled "Methods, Systems, and Computer Readable Media for Triggering a Service Node to Initiate a Session with a Policy Charging and Rules Function," filed on Mar. 15, 2011, Attorney Docket No. 1322-405-22-2, (Serial No. not yet assigned), herein incorporated by reference in its entirety, discloses the creation of such an external trigger by a PCRF node. The external trigger may include an IP address associated with UE 104.

[0029] At step 5, in response to the external trigger, service node 120 may send a message to PCRF node 114 which includes the IP address. The message may be sent, for example, via a Gx-Lite CCR-I Diameter message.

[0030] Table 1 illustrates an exemplary Gx-Lite CCR-I message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length "XXX" to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the r-bit set to "REQ" to indicate that the message is a request and the p-bit set to "PXY" to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID "YYYY" to

denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID "ZZZZZZZZ" to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0031] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the request. For example, Line 11 illustrates an origin host AVP corresponding with service node 120. The message may further include the origin realm AVP indicating the realm of the node that generated the request. For example, Line 12 illustrates an origin realm AVP indicating the realm of service node 120. The message may further include the destination realm AVP indicating the realm of the node the message is destined for. For example, Line 13 illustrates a destination realm AVP indicating the realm of PCRF node 114. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 14 illustrates the CC-request-type AVP corresponding with an initial request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 15 illustrates the CC-request-number AVP "0" denoting a first request.

[0032] The message may include an indication of the beginning of subscription information. For example, Line 16 illustrates an indication that subscription information is included. In some embodiments, PCRF node 114 may support receiving multiple subscription IDs in a single message. The message may further include the subscription-ID-type AVP for specifying the format of the subscription ID information. For example, Line 17 illustrates the subscription-ID-type AVP indicating that the subscription ID information is an end user IMSI. The message may further include the subscription-ID-data AVP for providing the subscription ID information itself. For example, Line 18 illustrates the subscription-ID-data AVP specifying the symbolic value "IMSI" to denote an IMSI associated with UE 104. The message may further include the supported-features AVP for informing the destination host of the features supported by the originating host. For example, Line 19 illustrates the supported-features AVP for informing PCRF node 114 of the features supported by service node 120. The message may further include the vendor-ID AVP for identifying the vendor of the originating host. For example, Line 20 illustrates the vendor-ID AVP specifying the vendor "Camiant" of service node 120. The message may further include the feature-list-ID AVP identifying the appropriate feature list from multiple possible supported feature lists. For example, Line 21 illustrates the feature-list-ID AVP indicating symbolic feature list "1" of multiple possible supported feature lists. The message may further include the feature-list AVP identifying the supported features. For example, Line 22 illustrates the feature-list AVP specifying features supported by service node 120 (e.g., "Gx-Lite"). The message may further include the framed-IP-ad-

dress AVP indicating an address to be configured for the user. The IP address specified may be, for example, a version 4 or version 6 address. For example, Line 23 illustrates the framed-IP-address AVP specifying an IP address associated with UE 104.

TABLE 1

01: Version	= 1
02: Message Length	= XXX
03: Command Flags	= REQ, PXY
04: Command Code	= Credit-control (272)
05: Application Id	= 16777238
06: Hop-By-Hop-Id	= YYYY
07: End-To-End-Id	= ZZZZZZZZ
08: AVPs	
09: Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10: Auth-Application-Id	= 16777238
11: Origin-Host	= NON-3GPP PCEF.Op.com
12: Origin-Realm	= Op.com
13: Destination-Realm	= Op.com
14: CC-Request-Type	= INITIAL_REQUEST (1)
15: CC-Request-Number	= 0
16: [Subscription-Id] // optional	
17: Subscription-Id-Type	= END_USER_IMSI (1)
18: Subscription-Id-Data	= <IMSI>
19: Supported-Features	
20: Vendor-Id	= Camiant (21274)
21: Feature-List-ID	= TBD [e.g., 1]
22: Feature-List	= TBD [e.g., Gx-Light]
23: Framed-IP-Address	= 192.168.2.11

[0033] Utilizing the IP address included in the CCR-I message, PCRF node 114 may determine a network access identifier (NAI) for a subscriber associated with UE 104. The NAI may be an international mobile station identifier (IMSI), a mobile subscriber integrated services digital network number (MSISDN), a uniform resource identifier (URI), an IMS public identity, or an IMS private identity. PCRF node 114 may query SDM node 118 in order to determine a NAI for the subscriber based on the IP address. In one embodiment, PCRF node 114 may utilize information derived from exchanges with PCEF node 116 to determine the NAI. For example, commonly owned, co-pending U.S. patent application entitled “Methods, Systems, and Computer Readable Media for Performing PCRF-Based User Information Pass Through,” filed on Mar. 15, 2011, Attorney Docket No. 1322-405-20-2, (Serial No. not yet assigned), herein incorporated by reference in its entirety, discloses an approach for providing a PCRF with user ID and/or IP address information.

[0034] Having determined a NAI for the subscriber associated with UE 104, PCRF node 114 may utilize the NAI to select an appropriate policy rule. The policy rule selected may authorize or de-authorize a content-filtering service and/or a web-optimization service for the subscriber associated with UE 104. The policy rule selected may specify user data plane content that is to be blocked for the subscriber associated with UE 104. For example, the policy rule may specify to block user data plane content associated with a uniform resource location (URL), a web page, a text string, an image, and/or a video. At step 6, PCRF node 114 may communicate the selected policy rule to service node 120 via a message. The message may be sent, for example, via a Gx-Lite CCA-I Diameter message.

[0035] Table 2 illustrates an exemplary Gx-Lite CCA-I message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message

may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length of the message illustrated. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0036] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include a result code AVP for reporting potential errors. For example, Line 10 illustrates the result code AVP “2001” indicating that the request was successfully completed. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the answer. For example, Line 11 illustrates an origin host AVP corresponding with PCRF node 114. The message may further include the origin realm AVP indicating the realm of the node that generated the answer. For example, Line 12 illustrates an origin realm AVP indicating the realm of PCRF node 114. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 13 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 14 illustrates the CC-request-type AVP corresponding with an initial request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 15 illustrates the CC-request-number AVP “0” denoting a first request.

[0037] The message may further include the supported-features AVP for informing the destination host of the features supported by the originating host. For example, Line 16 illustrates the supported-features AVP for informing service node 120 of the features supported by PCRF node 114. The message may further include the vendor-ID AVP for identifying the vendor of the originating host. For example, Line 17 illustrates the vendor-ID AVP specifying the vendor “Camiant” of PCRF node 114. The message may further include the feature-list-ID AVP identifying the appropriate feature list from multiple possible supported feature lists. For example, Line 18 illustrates the feature-list-ID AVP indicating symbolic feature list “1” of multiple possible supported feature

lists. The message may further include the feature-list AVP identifying the supported features. For example, Line 19 illustrates the feature-list AVP specifying features supported by PCRF node 114 (e.g., “Gx-Lite”). The message may further include the charging rule install AVP for specifying charging rules to be installed. For example, Line 20 illustrates the charging rule install AVP. The message may further include the charging rule name AVP and identify charging rules to install. Charging rules may be predefined or dynamic. For example, Lines 21 and 22 both illustrate the charging rule name AVP respectively specifying the predefined “Default_Traffic” charging rule and the predefined “P2P_Traffic” charging rule for installation at service node 120 with respect to UE 104’s IP CAN session.

TABLE 2

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Result-Code	= DIAMETER_SUCCESS (2001)
11:	Origin-Host	= pcrf1.Op.com
12:	Origin-Realm	= Op.com
13:	Auth-Application-Id	= 16777238
14:	CC-Request-Type	= INITIAL_REQUEST(1)
15:	CC-Request-Number	= 0
16:	Supported Features	
17:	Vendor-Id	= Camiant (21274)
18:	Feature-List-ID	= TBD [e.g., 1]
19:	Feature-List	= TBD [e.g., Gx-Lite]
20:	Charging-Rule-Install	
21:	Charging-Rule-Name	= Default-Traffic
22:	Charging-Rule-Name	= P2P_Traffic

[0038] Upon receiving the message from PCRF node 114, service node 120 may implement the policy rule(s) with respect to UE 104’s IP CAN session.

[0039] FIG. 3 is a message flow diagram illustrating an exemplary PCRF initiated termination of a session for communicating policy information according to an embodiment of the subject matter described herein. Referring to FIG. 3, an IP CAN session may exist between UE 104 and PCEF node 116 enabling UE 104 to communicate with a host in Internet 110. User data plane 300, carrying traffic associated with UE 104’s IP CAN session, may traverse service node 120. At step 1, UE 104 may initiate termination of the IP CAN session with PCEF node 116. At step 2, PCEF node 116 may send a credit-control-request termination (CCR-T) message to PCRF node 114. The CCR-T message may include a session ID identifying a session between PCEF node 116 and PCRF node 114 associated with UE 104’s IP CAN session. At step 3, PCRF node 114 may acknowledge PCEF node 116’s request by sending, to PCEF node 116, a credit-control-answer termination (CCA-T) message. The CCA-T message may include the session ID identifying the session between PCEF node 116 and PCRF node 114 associated with UE 104’s IP CAN session. PCEF node 116 may support an implementation of the full blown Gx protocol and thus the CCR-T/CCA-T exchange, between PCEF node 116 and PCRF node 114, may utilize the Gx protocol.

[0040] PCRF node 114 may desire to terminate an existing session with service node 120 associated with UE 104’s IP

CAN session. Service node 120 may not implement the full blown Gx protocol and thus utilization of the Gx protocol may not be possible. In accordance with embodiments of the subject matter described herein, PCRF node 114 may terminate the existing session with service node 120. For example, at step 4, PCRF node 114 may send a re-authorization-request (RAR) message to service node 120. The RAR message may include a session ID identifying a session between PCRF node 114 and service node 120 associated with UE 104’s IP CAN session and may further include a reason for terminating the session. The message may be sent, for example, via a Gx-Lite RAR Diameter message.

[0041] Table 3 illustrates an exemplary Gx-Lite RAR message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message’s length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the r-bit set to “REQ” to indicate that the message is a request and the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the re-authorization command code 258, corresponding with a re-authorization-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0042] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the request. For example, Line 11 illustrates an origin host AVP corresponding with PCRF node 114. The message may further include the origin realm AVP indicating the realm of the node that generated the request. For example, Line 12 illustrates an origin realm AVP indicating the realm of PCRF node 114. The message may further include the destination host AVP and convey the fully qualified domain name of the node the message is destined for. For example, Line 13 illustrates a destination host AVP corresponding with service node 120. The message may further include the destination realm AVP indicating the realm of the node the message is destined for. For example, Line 14 illustrates a destination

realm AVP indicating the realm of service node **120**. The message may further include the re-authorization request type AVP to inform the client of the action expected upon expiration of the authorization. For example, Line 15 illustrates the re-authorization request type AVP set to “AUTHORIZE_ONLY” to indicate the expiration of the authorization lifetime. The message may further include the session release cause AVP for indicating a reason for the termination. For example, Line 16 illustrates the session release cause AVP indicating an unspecified reason for the termination.

TABLE 3

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= REQ_PXY
04:	Command Code	= Re-Auth (258)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= pcrf1.Op.com
12:	Origin-Realm	= Op.com
13:	Destination-Host	= non-3GPP PCEF.Op.com
14:	Destination-Realm	= Op.com
15:	Re-Auth-Request-Type	= AUTHORIZE_ONLY
16:	Session-Release-Cause	= UNSPECIFIED_REASON

[0043] At step 5, service node **120** may acknowledge PCRF node **114**’s RAR message by sending a re-authorization-answer (RAA) message to PCRF node **114**. The message may be sent, for example, via a Gx-Lite RAA Diameter message.

[0044] Table 4 illustrates an exemplary Gx-Lite RAA message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message’s length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the re-authorization command code 258, corresponding with a re-authorization-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0045] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corre-

sponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the answer. For example, Line 11 illustrates an origin host AVP corresponding with service node **120**. The message may further include the origin realm AVP indicating the realm of the node that generated the answer. For example, Line 12 illustrates an origin realm AVP indicating the realm of service node **120**. The message may further include a result code AVP for reporting potential errors. For example, Line 13 illustrates the result code AVP “2001” indicating that the request was successfully completed.

TABLE 4

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= PXY
04:	Command Code	= Re-Auth (258)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= non-3GPP PCEF.Op.com
12:	Origin-Realm	= Op.com
13:	Result-Code	= DIAMETER_SUCCESS (2001)

[0046] At step 6, service node **120** may send a CCR-T message to PCRF node **114**. The message may be sent, for example, via a Gx-Lite CCR-T Diameter message.

[0047] Table 5 illustrates an exemplary Gx-Lite CCR-T message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message’s length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the r-bit set to “REQ” to indicate that the message is a request and the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0048] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the request. For example, Line 11 illustrates an origin host AVP corresponding with service node **120**. The message may further include the origin realm AVP indicating the realm of the node that generated the request. For example, Line 12 illustrates an origin realm AVP indicating the realm of the node the message is destined for. For example, Line 13 illustrates a destination realm AVP indicating the realm of PCRF node **114**. The message may further include the destination host AVP and convey the fully qualified domain name of the node the message is destined for. For example, Line 14 illustrates a destination host AVP corresponding with PCRF node **114**. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 15 illustrates the CC-request-type AVP corresponding with a termination request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 16 illustrates the CC-request-number AVP “1” denoting a first request. The message may further include the termination cause AVP containing information about the termination reason. For example, Line 17 illustrates a termination cause AVP specifying the termination reason as a Diameter logout.

TABLE 5

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= REQ, PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= NON-3GPP PCEF.Op.com
12:	Origin-Realm	= Op.com
13:	Destination-Realm	= Op.com
14:	Destination-Host	= pcrf1.Op.com
15:	CC-Request-Type	= TERMINATION_REQUEST (3)
16:	CC-Request-Number	= 1
17:	Termination-Cause	= DIAMETER_LOGOUT (1)

[0049] At step 7, PCRF node **114** may acknowledge service node **120**’s CCR-T message by sending a CCA-T message to service node **120**. The message may be sent, for example, via a Gx-Lite CCA-T Diameter message.

[0050] Table 6 illustrates an exemplary Gx-Lite CCA-T message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message’s length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length

of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0051] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the answer. For example, Line 11 illustrates an origin host AVP corresponding with PCRF node **114**. The message may further include the origin realm AVP indicating the realm of the node that generated the answer. For example, Line 12 illustrates an origin realm AVP indicating the realm of PCRF node **114**. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 13 illustrates the CC-request-type AVP corresponding with a termination request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 14 illustrates the CC-request-number AVP “1” denoting a first request. The message may further include a result code AVP for reporting potential errors. For example, Line 15 illustrates the result code AVP “2001” indicating that the request was successfully completed.

TABLE 6

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= pcrf1.Op.com
12:	Origin-Realm	= Op.com
13:	CC-Request-Type	= TERMINATION_REQUEST (3)
14:	CC-Request-Number	= 1
15:	Result-Code	= DIAMETER_SUCCESS (2001)

[0052] FIG. 4 is a message flow diagram illustrating an exemplary externally initiated termination of a session for communicating policy information according to an embodiment of the subject matter described herein. Referring to FIG. 4, an IP CAN session may exist between UE 104 and PCEF node 116 enabling UE 104 to communicate with a host in Internet 110. User data plane 400, carrying traffic associated with UE 104's IP CAN session, may traverse service node 120. Upon the occurrence of specified conditions, service node 120 may desire to terminate an existing session with PCRF node 114 associated with UE 104's IP CAN session. Service node 120 may not implement the full blown Gx protocol and thus utilization of the Gx protocol may not be possible. In accordance with embodiments of the subject matter described herein, service node 120 may terminate the existing session with PCRF node 114. For example, at step 1, a triggering event may occur at service node 120. For example, an inactivity timer associated with the session may expire. In response to the triggering event, at step 2, service node 120 may send a CCR-T message to PCRF node 114. The message may include a session ID identifying the session between service node 120 and PCRF node 114 associated with UE 104's IP CAN session. The message may be sent, for example, via a Gx-Lite CCR-T Diameter message.

[0053] Table 7 illustrates an exemplary Gx-Lite CCR-T message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length "XXX" to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the r-bit set to "REQ" to indicate that the message is a request and the p-bit set to "PXY" to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID "YYYY" to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID "ZZZZZZZZ" to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0054] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that

generated the request. For example, Line 11 illustrates an origin host AVP corresponding with service node 120. The message may further include the origin realm AVP indicating the realm of the node that generated the request. For example, Line 12 illustrates an origin realm AVP indicating the realm of service node 120. The message may further include the destination realm AVP indicating the realm of the node the message is destined for. For example, Line 13 illustrates a destination realm AVP indicating the realm of PCRF node 114. The message may further include the destination host AVP and convey the fully qualified domain name of the node the message is destined for. For example, Line 14 illustrates a destination host AVP corresponding with PCRF node 114. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 15 illustrates the CC-request-type AVP corresponding with a termination request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 16 illustrates the CC-request-number AVP "1" denoting a first request. The message may further include the termination cause AVP containing information about the termination reason. For example, Line 17 illustrates a termination cause AVP specifying the termination reason as a Diameter logout.

TABLE 7

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= REQ,PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= NON-3GPP PCEF.Op.com
12:	Origin-Realm	= Op.com
13:	Destination-Realm	= Op.com
14:	Destination-Host	= pcrf1.Op.com
15:	CC-Request-Type	= TERMINATION_REQUEST (3)
16:	CC-Request-Number	= 1
17:	Termination-Cause	= DIAMETER_LOGOUT (1)

[0055] At step 3, PCRF node 114 may acknowledge service node 120's CCR-T message by sending a CCA-T message to service node 120. The message may be sent, for example, via a Gx-Lite CCA-T Diameter message.

[0056] Table 8 illustrates an exemplary Gx-Lite CCA-T message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length "XXX" to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the p-bit set to "PXY" to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet

vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0057] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the answer. For example, Line 11 illustrates an origin host AVP corresponding with PCRF node 114. The message may further include the origin realm AVP indicating the realm of the node that generated the answer. For example, Line 12 illustrates an origin realm AVP indicating the realm of PCRF node 114. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 13 illustrates the CC-request-type AVP corresponding with a termination request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 14 illustrates the CC-request-number AVP “1” denoting a first request. The message may further include a result code AVP for reporting potential errors. For example, Line 15 illustrates the result code AVP “2001” indicating that the request was successfully completed.

TABLE 8

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= pcrf1.Op.com
12:	Origin-Realm	= Op.com
13:	CC-Request-Type	= TERMINATION_REQUEST (3)
14:	CC-Request-Number	= 1
15:	Result-Code	= DIAMETER_SUCCESS (2001)

[0058] FIG. 5 is a message flow diagram illustrating an exemplary policy rule push for communicating policy information according to an embodiment of the subject matter described herein. Referring to FIG. 5, an IP CAN session may exist between UE 104 and PCEF node 116 enabling UE 104 to communicate with a host in Internet 110. User data plane 500, carrying traffic associated with UE 104’s IP CAN session, may traverse service node 120. Upon the occurrence of specified conditions, PCRF node 114 may desire to push a policy rule update associated with UE 104’s IP CAN session

to service node 120. Service node 120 may not implement the full blown Gx protocol and thus utilization of the Gx protocol may not be possible. In accordance with embodiments of the subject matter described herein, PCRF node 114 may push a policy rule update associated with UE 104’s IP CAN session to service node 120. For example, at step 1, a triggering event may occur at PCRF node 114. For example, a time-of-day condition may occur at PCRF node 114. In response to the triggering event, at step 2, PCRF node 114 may send a RAR message to service node 120. The message may include a session ID identifying the session between service node 120 and PCRF node 114 associated with UE 104’s IP CAN session. The message may further include a charging rule(s) update for service node 120 to implement with respect to UE 104’s IP CAN session. The message may be sent, for example, via a Gx-Lite RAR Diameter message.

[0059] Table 9 illustrates an exemplary Gx-Lite RAR message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message’s length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length of the message illustrated. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the r-bit set to “REQ” to indicate that the message is a request and the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the re-authorization command code 258, corresponding with a re-authorization-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0060] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the request. For example, Line 11 illustrates an origin host AVP corresponding with PCRF node 114. The message may further include the origin realm AVP indicating the realm of the node that generated the request. For example, Line 12 illustrates an origin realm AVP indicating the realm of PCRF node 114. The message may further include the destination host AVP and convey the fully qualified domain name of the node the message is destined for. For example, Line 13

illustrates a destination host AVP corresponding with service node **120**. The message may further include the destination realm AVP indicating the realm of the node the message is destined for. For example, Line 14 illustrates a destination realm AVP indicating the realm of service node **120**. The message may further include the re-authorization request type AVP to inform the client of the action expected upon expiration of the authorization. For example, Line 15 illustrates the re-authorization request type AVP set to "AUTHORIZE_ONLY" to indicate the expiration of the authorization lifetime. The message may further include the charging rule remove AVP for specifying charging rules to be uninstalled. For example, Line 16 illustrates the charging rule remove AVP. The message may further include the charging rule name AVP and identify a charging rule to remove. The charging rule may be predefined or dynamic. For example, Line 17 illustrates the charging rule name AVP specifying the predefined "normal_bw_p2p" charging rule for removal at service node **120** with respect to UE **104**'s IP CAN session. The message may further include the charging rule install AVP for specifying charging rules to be installed. For example, Line 18 illustrates the charging rule install AVP. The message may further include the charging rule name AVP and identify a charging rule to install. The charging rule may be predefined or dynamic. For example, Line 19 illustrates the charging rule name AVP specifying the predefined "happyHour_bw_p2p" charging rule for installation at service node **120** with respect to UE **104**'s IP CAN session.

TABLE 9

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= REQ, PXY
04:	Command Code	= Re-Auth (258)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= pcrf1.Op.com
12:	Origin-Realm	= Op.com
13:	Destination-Host	= non-3GPP PCEF.Op.com
14:	Destination-Realm	= Op.com
15:	Re-Auth-Request-Type	= AUTHORIZE_ONLY
16:	[Charging-Rule-Remove]	
17:	Charging-Rule-Name	= normal_bw_p2p
18:	[Charging-Rule-Install]	
19:	Charging-Rule-Name	= happyHour_bw_p2p

[0061] Service node **120** may then install the charging rule (s) update (i.e., uninstall the "normal_bw_p2p" charging rule and install the "happyHour_bw_p2p" charging rule) with respect to UE **104**'s IP CAN session.

[0062] At step 3, service node **120** may acknowledge PCRF node **114**'s RAR message by sending a RAA message to PCRF node **114**. The message may be sent, for example, via a Gx-Lite RAA Diameter message.

[0063] Table 10 illustrates an exemplary Gx-Lite RAA message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length "XXX" to denote the length

of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the p-bit set to "PXY" to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the re-authorization command code 258, corresponding with a re-authorization-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID "YYYY" to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID "ZZZZZZZZ" to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0064] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the answer. For example, Line 11 illustrates an origin host AVP corresponding with service node **120**. The message may further include the origin realm AVP indicating the realm of the node that generated the answer. For example, Line 12 illustrates an origin realm AVP indicating the realm of service node **120**. The message may further include a result code AVP for reporting potential errors. For example, Line 13 illustrates the result code AVP "2001" indicating that the request was successfully completed.

TABLE 10

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= PXY
04:	Command Code	= Re-Auth (258)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= non-3GPP PCEF.Op.com
12:	Origin-Realm	= Op.com
13:	Result-Code	= DIAMETER_SUCCESS (2001)

[0065] FIG. 6 is a message flow diagram illustrating an exemplary audit procedure for communicating policy information according to an embodiment of the subject matter described herein. Referring to FIG. 6, an IP CAN session may exist between UE **104** and PCEF node **116** enabling UE **104** to communicate with a host in Internet **110**. User data plane **600**, carrying traffic associated with UE **104**'s IP CAN session, may traverse service node **120**. Upon the occurrence of specified conditions, PCRF node **114** may desire to determine

whether a session between itself and service node 120 associated with UE 104's IP CAN session remains active or has become inactive. Service node 120 may not implement the full blown Gx protocol and thus utilization of the Gx protocol may not be possible. In accordance with embodiments of the subject matter described herein, PCRF node 114 may determine whether a session between itself and service node 120 associated with UE 104's IP CAN session remains active or has become inactive. For example, at step 1, a triggering event may occur at PCRF node 114. For example, a periodic audit condition may occur at PCRF node 114. In response to the triggering event, at step 2, PCRF node 114 may send a RAR message to service node 120. The message may include a session ID identifying the session between service node 120 and PCRF node 114 associated with UE 104's IP CAN session. The message may be sent, for example, via a Gx-Lite RAR Diameter message.

[0066] Table 11 illustrates an exemplary Gx-Lite RAR message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length "XXX" to denote the length of the message illustrated. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the r-bit set to "REQ" to indicate that the message is a request and the p-bit set to "PXY" to indicate that the message is proxiabable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the re-authorization command code 258, corresponding with a re-authorization-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID "YYYY" to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID "ZZZZZZZZ" to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0067] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the request. For example, Line 11 illustrates an origin host AVP corresponding with PCRF node 114. The message may further include the origin realm AVP indicating the realm of the node that generated the request. For example, Line 12 illustrates an origin realm AVP indicating the realm of PCRF node 114. The message may further include the desti-

nation host AVP and convey the fully qualified domain name of the node the message is destined for. For example, Line 13 illustrates a destination host AVP corresponding with service node 120. The message may further include the destination realm AVP indicating the realm of the node the message is destined for. For example, Line 14 illustrates a destination realm AVP indicating the realm of service node 120. The message may further include the re-authorization request type AVP to inform the client of the action expected upon expiration of the authorization. For example, Line 15 illustrates the re-authorization request type AVP set to "AUTHORIZE_ONLY" to indicate the expiration of the authorization lifetime.

TABLE 11

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= REQ, PXY
04:	Command Code	= Re-Auth (258)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= pcrf1.Op.com
12:	Origin-Realm	= Op.com
13:	Destination-Host	= non-3GPP PCEF.Op.com
14:	Destination-Realm	= Op.com
15:	Re-Auth-Request-Type	= AUTHORIZE_ONLY

[0068] At step 3, service node 120 may acknowledge PCRF node 114's RAR message by sending a RAA message to PCRF node 114. The message may include a result code indicating whether the session remains active or has become inactive. The message may be sent, for example, via a Gx-Lite RAA Diameter message.

[0069] Table 12 illustrates an exemplary Gx-Lite RAA message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length "XXX" to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the p-bit set to "PXY" to indicate that the message is proxiabable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the re-authorization command code 258, corresponding with a re-authorization-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID "YYYY" to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID "ZZZZZZZZ" to denote a unique end-to-end ID. The message may further include the

AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0070] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the answer. For example, Line 11 illustrates an origin host AVP corresponding with service node 120. The message may further include the origin realm AVP indicating the realm of the node that generated the answer. For example, Line 12 illustrates an origin realm AVP indicating the realm of service node 120. The message may further include if/else decisional logic surrounding result code AVPs for reporting potential errors that may correspond with whether the session remains active or has become inactive. For example, Lines 13-16 illustrate pseudo code for if/else decisional logic that will invoke the result code AVP “2001” indicating that the request was successfully completed if the session remains active and will invoke the result code AVP “5002” indicating that the request contained an unknown session ID if the session has become inactive.

TABLE 12

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= PXY
04:	Command Code	= Re-Auth (258)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= non-3GPP PCEF.Op.com
12:	Origin-Realm	= Op.com
13:	if the session exists then	
14:	Result-Code	= DIAMETER_SUCCESS (2001)
15:	else	
16:	Result-Code	= DIAMETER_UNKNOWN_SESSION_ID (5002)

[0071] In response to service node 120’s RAA message indicating that the session has become inactive, PCRF node 114 may invoke procedures to free up resources associated with the session.

[0072] FIG. 7 is a message flow diagram illustrating exemplary event subscription and notification for communicating policy information according to an embodiment of the subject matter described herein. Referring to FIG. 7, at step 1, UE 104 may initiate establishment of an IP CAN session with PCEF node 116 for the purpose of communicating with a host in Internet 110. At step 2, PCEF node 116 may send a CCR message to PCRF node 114. The CCR message may include a user ID and IP address associated with UE 104. At step 3, PCRF node 114 may send a CCA message to PCEF node 116. The CCA message may include a charging rule for PCEF node 116 to implement with respect to UE 104’s IP CAN session. PCEF node 116 may support an implementation of

the full blown Gx protocol and thus the CCR/CCA exchange, between PCEF node 116 and PCRF node 114, may utilize the Gx protocol.

[0073] User data plane 700, carrying traffic associated with UE 104’s IP CAN session, may traverse service node 120. PCRF node 114 may desire to communicate with service node 120 in order to subscribe to SDF event notifications and/or install policy rule(s). Service node 120 may not implement the full blown Gx protocol and thus utilization of the Gx protocol may not be possible. In accordance with embodiments of the subject matter described herein, PCRF node 114 may communicate with service node 120 in order to subscribe to SDF event notifications and/or install policy rule(s).

[0074] At step 4, service node 120 may receive an external trigger indicating that it should establish a session with PCRF node 114. The external trigger may include an IP address associated with UE 104. At step 5, in response to the external trigger, service node 120 may send a message to PCRF node 114 which includes the IP address. The message may be sent, for example, via a Gx-Lite CCR-I Diameter message.

[0075] Table 13 illustrates an exemplary Gx-Lite CCR-I message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message’s length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the r-bit set to “REQ” to indicate that the message is a request and the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0076] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the request. For example, Line 11 illustrates an origin host AVP corresponding with service node 120. The message may further include the origin realm AVP indicating the realm of the node that generated the request. For example,

Line 12 illustrates an origin realm AVP indicating the realm of service node **120**. The message may further include the destination realm AVP indicating the realm of the node the message is destined for. For example, Line 13 illustrates a destination realm AVP indicating the realm of PCRF node **114**. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 14 illustrates the CC-request-type AVP corresponding with an initial request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 15 illustrates the CC-request-number AVP “0” denoting a first request.

[0077] The message may include an indication of the beginning of subscription information. For example, Line 16 illustrates an indication that subscription information is included. In some embodiments, PCRF node **114** may support receiving multiple subscription IDs in a single message. The message may further include the subscription-ID-type AVP for specifying the format of the subscription ID information. For example, Line 17 illustrates the subscription-ID-type AVP indicating that the subscription ID information is an end user IMSI. The message may further include the subscription-ID-data AVP for providing the subscription ID information itself. For example, Line 18 illustrates the subscription-ID-data AVP specifying the symbolic value “IMSI” to denote an IMSI associated with UE **104**. The message may further include the supported-features AVP for informing the destination host of the features supported by the originating host. For example, Line 19 illustrates the supported-features AVP for informing PCRF node **114** of the features supported by service node **120**. The message may further include the vendor-ID AVP for identifying the vendor of the originating host. For example, Line 20 illustrates the vendor-ID AVP specifying the vendor “Camiant” of service node **120**. The message may further include the feature-list-ID AVP identifying the appropriate feature list from multiple possible supported feature lists. For example, Line 21 illustrates the feature-list-ID AVP indicating symbolic feature list “1” of multiple possible supported feature lists. The message may further include the feature-list AVP identifying the supported features. For example, Line 22 illustrates the feature-list AVP specifying features supported by service node **120** (e.g., “Gx-Lite”). The message may further include the framed-IP-address AVP indicating an address to be configured for the user. The IP address specified may be, for example, a version 4 or version 6 address. For example, Line 23 illustrates the framed-IP-address AVP specifying an IP address associated with UE **104**.

TABLE 13

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= REQ, PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= NON-3GPP PCEF.Op.com
12:	Origin-Realm	= Op.com
13:	Destination-Realm	= Op.com
14:	CC-Request-Type	= INITIAL_REQUEST (1)
15:	CC-Request-Number	= 0

TABLE 13-continued

16:	[Subscription-Id] // optional	
17:	Subscription-Id-Type	= END_USER_IMSI (1)
18:	Subscription-Id-Data	= <IMSI>
19:	Supported-Features	
20:	Vendor-Id	= Camiant (21274)
21:	Feature-List-ID	= TBD [e.g., 1]
22:	Feature-List	= TBD [e.g., Gx-Lite]
23:	Framed-IP-Address	= 192.168.2.11

[0078] Utilizing the IP address included in the CCR-I message, PCRF node **114** may determine a NAI for a subscriber associated with UE **104**. The NAI may be an IMSI, a MSISDN, a URI, an IMS public identity, or an IMS private identity. PCRF node **114** may query SDM node **118** in order to determine a NAI for the subscriber based on the IP address. In one embodiment, PCRF node **114** may utilize information derived from exchanges with PCEF node **116** to determine the NAI.

[0079] Having determined a NAI for the subscriber associated with UE **104**, PCRF node **114** may utilize the NAI to select an appropriate policy rule. The policy rule selected may authorize or de-authorize a content-filtering service and/or a web-optimization service for the subscriber associated with UE **104**. The policy rule selected may specify user data plane content that is to be blocked for the subscriber associated with UE **104**. For example, the policy rule may specify to block user data plane content associated with a URL, a web page, a text string, an image, and/or a video. Additionally, PCRF node **114** may determine that it should be notified upon the detection of an SDF event by service node **120** and that it should therefore subscribe to the appropriate SDF detection. At step 6, PCRF node **114** may communicate the selected policy rule and/or the SDF detection subscription to service node **120** via a message. The message may be sent, for example, via a Gx-Lite CCA-I Diameter message.

[0080] Table 14 illustrates an exemplary Gx-Lite CCA-I message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the

AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0081] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include a result code AVP for reporting potential errors. For example, Line 10 illustrates the result code AVP “2001” indicating that the request was successfully completed. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the answer. For example, Line 11 illustrates an origin host AVP corresponding with PCRF node **114**. The message may further include the origin realm AVP indicating the realm of the node that generated the answer. For example, Line 12 illustrates an origin realm AVP indicating the realm of PCRF node **114**. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 13 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 14 illustrates the CC-request-type AVP corresponding with an initial request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 15 illustrates the CC-request-number AVP “0” denoting a first request. The message may further include the event trigger AVP for identifying a specified event that should cause service node **120** to re-request PCC rule(s). For example, Line 16 illustrates the event trigger AVP and indicates that service node **120** should re-request PCC rule(s) upon SDF detection. The message may further include the charging rule install AVP for specifying charging rule(s) to be installed. For example, Line 17 illustrates the charging rule install AVP. The message may further include the charging rule name AVP and identify a charging rule(s) to install. A charging rule may be predefined or dynamic. For example, Line 18 illustrates the charging rule name AVP specifying the predefined “Default_Traffic” charging rule for installation at service node **120** with respect to UE **104**’s IP CAN session. The message may further include an additional charging rule install AVP for specifying additional charging rule(s) to be installed. For example, Line 19 illustrates an additional charging rule install AVP. The message may further include additional charging rule name AVP(s) and identify the additional charging rule(s) to install. For example, Line 20 illustrates an additional charging rule name AVP specifying the predefined “P2P_Traffic” charging rule for installation at service node **120** with respect to UE **104**’s IP CAN session. The message may further include the service flow detection AVP for enabling SDF event detection. For example, Line 21 illustrates a service flow detection AVP for enabling SDF event detection.

TABLE 14

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	

TABLE 14-continued

09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Result-Code	= DIAMETER_SUCCESS (2001)
11:	Origin-Host	= perfl.Op.com
12:	Origin-Realm	= Op.com
13:	Auth-Application-Id	= 16777238
14:	CC-Request-Type	= INITIAL_REQUEST (1)
15:	CC-Request-Number	= 0
16:	Event-Trigger	= SERVICE_FLOW_DETECTION (1002)
17:	Charging-Rule-Install	
18:	Charging-Rule-Name	= Default_Traffic
19:	Charging-Rule-Install	
20:	Charging-Rule-Name	= P2P_Traffic
21:	Service-Flow-Detection	= ENABLE_DETECTION(0)

[0082] At step 7, service node **120** may detect the SDF event specified in the message received from PCRF node **114**. At step 8, service node **120** may send a credit-control-request update (CCR-U) message to PCRF node **114** indicating that the SDF event has been detected and re-requesting policy rule(s). The message may be sent, for example, via a Gx-Lite CCR-U Diameter message.

[0083] Table 15 illustrates an exemplary Gx-Lite CCR-U message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message’s length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length “XXX” to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the r-bit set to “REQ” to indicate that the message is a request and the p-bit set to “PXY” to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID “YYYY” to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID “ZZZZZZZZ” to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0084] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the request. For example, Line 11 illustrates an

origin host AVP corresponding with service node 120. The message may further include the destination host AVP and convey the fully qualified domain name of the node the message is destined for. For example, Line 12 illustrates a destination host AVP corresponding with PCRF node 114. The message may further include the origin realm AVP indicating the realm of the node that generated the request. For example, Line 13 illustrates an origin realm AVP indicating the realm of service node 120. The message may further include the destination realm AVP indicating the realm of the node the message is destined for. For example, Line 14 illustrates a destination realm AVP indicating the realm of PCRF node 114. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 15 illustrates the CC-request-type AVP corresponding with an update request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 16 illustrates the CC-request-number AVP "1" denoting an update request. The message may further include the origin state ID AVP for enabling other Diameter entities to infer that other sessions (i.e., sessions with a lower origin state ID) are no longer active. For example, Line 17 illustrates the origin state ID AVP indicating that sessions with an origin state ID lower than "1164772302" are no longer active. The message may further include the event trigger AVP for identifying the event trigger. For example, Line 18 illustrates the event trigger AVP and identifies the event trigger SDF detection. The message may further include the charging rule report AVP for indicating the beginning of the charging rule report. For example, Line 19 illustrates the charging rule report AVP and indicates the beginning of a charging rule report associated with the SDF detection. The message may further include the charging rule name AVP and identify a charging rule(s) associated with the report. For example, Line 20 illustrates the charging rule name AVP specifying the "P2P_Traffic" charging rule associated with the report. The message may further include the PCC rule status AVP for reporting the current status of the PCC rule. For example, Line 21 illustrates the PCC rule status AVP and reports the current status of the "P2P_Traffic" rule as active.

TABLE 15

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= REQ, PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= NON-3GPP PCEF.Op.com
12:	Destination-Host	= pcrf1.Op.com
13:	Origin-Realm	= Op.com
14:	Destination-Realm	= Op.com
15:	CC-Request-Type	= UPDATE_REQUEST (2)
16:	CC-Request-Number	= 1
17:	Origin-State-Id	= 1164772302
18:	Event-Trigger	= SERVICE_FLOW_DETECTION (1002)
19:	Charging-Rule-Report	=
20:	Charging-Rule-Name	= P2P_Traffic
21:	PCC-Rule-Status	= Active (0)

[0085] In response to receiving service node 120's CCR-U message, at step 9, PCRF node 114 may send a credit-control-answer update (CCA-U) message to service node 120. The message may include a charging rule(s) update for service node 120 to implement with respect to UE 104's IP CAN session. The message may be sent, for example, via a Gx-Lite CCA-U Diameter message.

[0086] Table 16 illustrates an exemplary Gx-Lite CCA-U message. The message may include the version field for specifying version information. For example, Line 1 illustrates the version field specifying version 1.0. The message may further include the message length field for specifying the message's length, including any header information. For example, Line 2 illustrates the message length field specifying the symbolic message length "XXX" to denote the length of the message. The message may further include the command flags field. For example, Line 3 illustrates the command flags field with the p-bit set to "PXY" to indicate that the message is proxiable. The message may further include the command codes field. For example, Line 4 illustrates the command codes field with the credit-control command code 272, corresponding with a credit-control-request. The message may further include the application ID field to identify to which application the message is applicable. For example, Line 5 illustrates the application ID field with a four octet vendor specific application ID. The message may further include a hop-by-hop ID field to aid in matching requests and replies. For example, Line 6 illustrates the hop-by-hop ID field specifying a symbolic hop-by-hop ID "YYYY" to denote a unique hop-by-hop ID. The message may further include an end-to-end ID field for detecting duplicate messages. For example, Line 7 illustrates an end-to-end ID field specifying a symbolic end-to-end ID "ZZZZZZZZ" to denote a unique end-to-end ID. The message may further include the AVPs field for indicating the beginning of AVPs. For example, Line 8 illustrates the AVPs field.

[0087] AVPs may be used to encapsulate information relevant to the message. The message may include a session ID AVP. For example, Line 9 illustrates a session ID AVP corresponding with the global identifier of the session. The message may further include an authentication application ID AVP or an accounting application ID AVP. For example, Line 10 illustrates an authentication ID AVP identifying the authentication and authorization portion of the application. The message may further include the origin host AVP and convey the fully qualified domain name of the node that generated the answer. For example, Line 11 illustrates an origin host AVP corresponding with PCRF node 114. The message may further include the origin realm AVP indicating the realm of the node that generated the answer. For example, Line 12 illustrates an origin realm AVP indicating the realm of PCRF node 114. The message may further include the CC-request-type AVP indicating the type of credit control request. For example, Line 15 illustrates the CC-request-type AVP corresponding with an update request. The message may further include the CC-request-number AVP indicating the credit control request number. For example, Line 16 illustrates the CC-request-number AVP "1" denoting an update request. The message may further include a result code AVP for reporting potential errors. For example, Line 15 illustrates the result code AVP "2001" indicating that the request was successfully completed. The message may further include the charging rule remove AVP for specifying charging rules to be uninstalled. For example, Line 16 illustrates the charging rule

remove AVP. The message may further include the charging rule name AVP and identify a charging rule to remove. The charging rule may be predefined or dynamic. For example, Line 17 illustrates the charging rule name AVP specifying the predefined “P2P-Traffic” charging rule for removal at service node **120** with respect to UE **104**’s IP CAN session. The message may further include the charging rule install AVP for specifying charging rules to be installed. For example, Line 18 illustrates the charging rule install AVP. The message may further include the charging rule name AVP and identify a charging rule to install. The charging rule may be predefined or dynamic. For example, Line 19 illustrates the charging rule name AVP specifying the predefined “block_p2p” charging rule for installation at service node **120** with respect to UE **104**’s IP CAN session.

TABLE 16

01:	Version	= 1
02:	Message Length	= XXX
03:	Command Flags	= PXY
04:	Command Code	= Credit-control (272)
05:	Application Id	= 16777238
06:	Hop-By-Hop-Id	= YYYY
07:	End-To-End-Id	= ZZZZZZZZ
08:	AVPs	
09:	Session-Id	= NON-3GPP PCEF.Op.com; 1876543210;102
10:	Auth-Application-Id	= 16777238
11:	Origin-Host	= pcrf1.Op.com
12:	Origin-Realm	= Op.com
13:	CC-Request-Type	= UPDATE_REQUEST (2)
14:	CC-Request-Number	= 1
15:	Result-Code	= DIAMETER_SUCCESS (2001)
16:	Charging-Rule-Remove	
17:	Charging-Rule-Name	= P2P-Traffic
18:	Charging-Rule-Install	
19:	Charging-Rule-Name	= block_p2p

[0088] Service node **120** may then install the charging rule (s) update (i.e., uninstall the “P2P-Traffic” charging rule and install the “block_p2p” charging rule) with respect to UE **104**’s IP CAN session.

[0089] FIG. **8** is a flow chart illustrating an exemplary process for communicating policy information according to an embodiment of the subject matter described herein. Referring to FIG. **8**, in step **800**, a PCRF node receives, from a service node, a message requesting a policy rule, wherein the message includes an IP address, associated with a subscriber. For example, PCRF node **114** may receive, from service node **120**, a message requesting a policy rule. The message may include an IP address associated with a subscriber utilizing UE **104**. The message may be, for example, a CCR-I message similar to that illustrated in Table 1. In step **802**, the PCRF node determines a NAI for the subscriber based on the IP address. For example, PCRF node **114** may determine a NAI for the subscriber utilizing UE **104** based on the IP address included in the received message. In step **804**, the PCRF node selects a policy rule for the subscriber based on the NAI. For example, PCRF node **114** may select a policy rule (i.e., “P2P-Traffic”) based on the NAI determined in step **802**. In step **806**, the PCRF node communicates the policy rule to the service node. For example, PCRF node **114** may communicate the “P2P-Traffic” rule to service node **120** via a CCA-I message similar to the message illustrated in Table 2.

[0090] FIG. **9** is a block diagram of an exemplary PCRF node for communicating policy information according to an embodiment of the subject matter described herein. Referring

to FIG. **9**, PCRF node **114** includes a communication interface **900** for sending and receiving messages. Communication interface **900** may be capable of communicating with other nodes via any suitable interface, such as a Gx interface, a Gxx interface, a Gx-Lite interface, or an Rx interface. PCRF node **114** further includes a communication module **902** configured to utilize communication interface **900** to receive, from a service node, a message requesting a policy rule, wherein the message includes an IP address associated with a subscriber. For example, communication module **902** may be configured to utilize communication interface **900** to receive, from service node **120**, a message requesting a policy rule, wherein the message includes an IP address associated with a subscriber utilizing UE **104**. For example, communication module **902** may be configured to utilize communication interface **900** to receive a message similar to the CCR-I message illustrated in Table 1. Communication module **902** is further configured to determine a NAI for the subscriber based on the IP address. For example, communication module **902** may be configured to determine a NAI for the subscriber utilizing UE **104**. Communication module **902** is further configured to select a policy rule for the subscriber based on the NAI. For example, communication module **902** may be configured to select a policy rule (e.g., “P2P-Traffic”) for the subscriber utilizing UE **104** based on the determined NAI. Communication module **902** is further configured to utilize communication interface **900** to communicate the policy rule to the service node. For example, communication module **902** may be configured to utilize communication interface **900** to communicate the “P2P-Traffic” policy rule to service node **120**. For example, communication module **902** may be configured to utilize communication interface **900** to communicate a message similar to the CCA-I message illustrated in Table 2.

[0091] It will be understood that various details of the subject matter described herein may be changed without departing from the scope of the subject matter described herein. Furthermore, the foregoing description is for the purpose of illustration only, and not for the purpose of limitation, as the subject matter described herein is defined by the claims as set forth hereinafter.

What is claimed is:

1. A method for communicating policy information, the method comprising:

at a policy charging and rules function (PCRF) node:

- receiving, from a service node, a message requesting a policy rule, wherein the message includes an Internet protocol (IP) address associated with a subscriber;
- determining a network access identifier (NAI) for the subscriber based on the IP address;
- selecting a policy rule for the subscriber based on the NAI; and
- communicating the policy rule to the service node.

2. The method of claim 1 wherein the NAI comprises at least one of an international mobile station identifier (IMSI), a mobile subscriber integrated services digital network number (MSISDN), a uniform resource identifier (URI), an Internet protocol (IP) multimedia subsystem (IMS) public identity, and an IMS private identity.

3. The method of claim 1 wherein determining the NAI for the subscriber comprises querying a subscriber data management (SDM) node.

4. The method of claim 3 wherein the SDM node comprises at least one of a home subscriber server (HSS), a user profile serving function (UPSF), and a subscription profile repository (SPR).

5. The method of claim 1 wherein the message comprises a Diameter message.

6. The method of claim 1 wherein the policy rule is communicated via a Diameter message.

7. The method of claim 1 wherein the message is received via an interface that implements a subset of a Gx protocol or Gx application.

8. The method of claim 1 wherein the policy rule is communicated via an interface that implements a subset of a Gx protocol or Gx application.

9. The method of claim 1 wherein the policy rule authorizes or de-authorizes at least one of a content-filtering service for the subscriber and a web-optimization service for the subscriber.

10. The method of claim 1 wherein the policy rule specifies user data plane content that is to be blocked for the subscriber.

11. A system for communicating policy information, the system comprising:

a policy and charging rules function (PCRF) node, the PCRF node comprising:

a communication interface; and

a communication module configured to:

utilize the communication interface to receive, from a service node, a message requesting a policy rule, wherein the message includes an Internet protocol (IP) address associated with a subscriber;

determine a network access identifier (NAI) for the subscriber based on the IP address;

select a policy rule for the subscriber based on the NAI; and

utilize the communication interface to communicate the policy rule to the service node.

12. The system of claim 11 wherein the NAI comprises at least one of an international mobile station identifier (IMSI), a mobile subscriber integrated services digital network number (MSISDN), a uniform resource identifier (URI), an Inter-

net protocol (IP) multimedia subsystem (IMS) public identity, and an IMS private identity.

13. The system of claim 12 wherein the communications module is configured to determine the NAI for the subscriber by querying a subscriber data management (SDM) node.

14. The system of claim 13 wherein the SDM node comprises at least one of a home subscriber server (HSS), a user profile serving function (UPSF), and a subscription profile repository (SPR).

15. The system of claim 11 wherein the message composes a Diameter message.

16. The system of claim 11 wherein the communication module is configured to receive the message via the communication interface by implementing a subset of a Gx protocol or Gx application.

17. The system of claim 11 wherein the communication module is configured to communicate the policy rule via the communication interface by implementing a subset of a Gx protocol or Gx application.

18. The system of claim 11 wherein the policy rule authorizes or de-authorizes at least one of a content-filtering service for the subscriber and a web-optimization service for the subscriber.

19. The system of claim 11 wherein the policy rule specifies user data plane content that is to be blocked for the subscriber.

20. A non-transitory computer readable medium comprising computer executable instructions that when executed by a processor of a computer control the computer to perform steps comprising:

receiving, from a service node, a message requesting a policy rule, wherein the message includes an Internet protocol (IP) address associated with a subscriber;

determining a network access identifier (NAI) for the subscriber based on the IP address;

selecting a policy rule for the subscriber based on the NAI; and

communicating the policy rule to the service node.

* * * * *