Open Access to Resource Management in Multimedia Networks

Evelina Nikolova Pencheva and Ivaylo Ivanov Atanasov
Faculty of Telecommunications, Technical University of Sofia, Bulgaria

***Abstract*— The paper is dedicated to mechanisms for open access to resource management in the Internet Protocol (IP) multimedia networks. First we present the concept of IP Multimedia Subsystem (IMS) and explain the IMS functional architecture, principles of quality of service management and service control in IMS. Then we describe the idea behind the opening of network interfaces for third parties so that others besides the network operator can create and deploy services. Open Service Access (OSA) and Parlay appear to be the technologies for value-added service delivery in multimedia networks. In the paper we take a closer look to the Parlay/OSA interfaces that allow third party applications to access the resource management functions in IMS. OSA "Connectivity Manager" interfaces and OSA "Policy Management" interfaces are considered. Parlay X Web Services interfaces provide a higher level of abstraction than Parlay/OSA interfaces and gain an amazing amount of support among service developers. We address "Application-driven Quality of Service" Parlay X Web Service and "Policy" Parlay X Web Service also.**

***Index Terms*—Internet Protocol Multimedia Subsystem (IMS), Quality of service management, Open Service Access, Parlay X**

I. INTRODUCTION

A. Internet Protocol Multimedia Subsystem concept

Internet Protocol Multimedia Subsystem (IMS) was born as an architectural framework for service delivering in third generation mobile networks. Now it is adopted by next generation networks as a key technology for fixed-mobile convergence.

The IMS is all about services. It enables operators to offer multimedia services based on and built upon Internet applications, services and protocols. IMS facilitates convergence of and access to voice, video, messaging, data and web-based technologies [1], [2]. One of the main principles behind the IMS shown in Fig.1 is access independence. It allows services to be provided over any network that supports IP.

IMS facilitates efficient introduction of new multimedia services. The services themselves are not standardizes but tailored to customer needs. Service customization is achieved by the use of service capabilities in both networks and terminals. The service capabilities are service component that can be used to create IP multimedia applications.

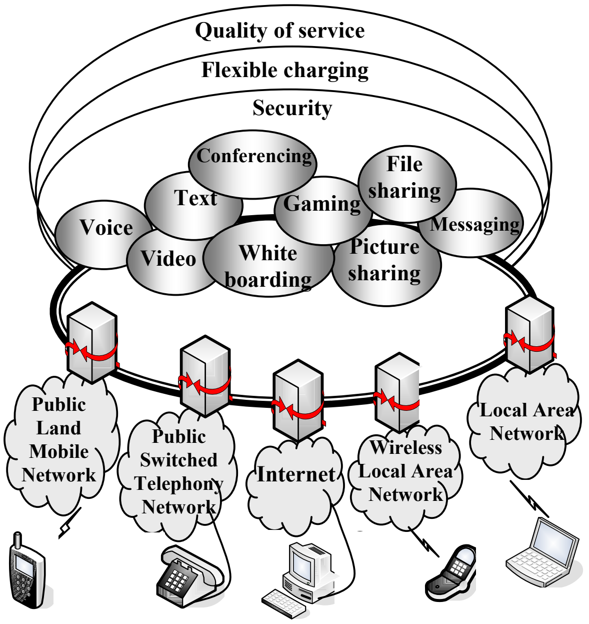


Fig.1 The IMS – All IP core network multimedia domain

B. IMS functional architecture

The layering approach is used to define the IMS architecture [3]. The IMS consists of three separate planes: User plane, Control plane and Application plane. Fig.2 shows IMS functions defined at the three layers.

The User plane is composed of traffic caring network elements like switches, routers, media gateways and access elements at the borders of the core network. The Policy and Charging Enforcement Function (PCEF) encompasses service data flow detection, policy enforcement and flow based charging functionalities. This PCEF is located at the media gateway. The media gateway provides service data flow detection, user traffic handling, triggering control plane session management, quality of service handling, and service data flow measurement as well as online and offline charging interactions. The User plane also contains Media Resource Function Processor (MRFP) providing media resources for playing announcements and conferencing.

The Control plane comprises control servers. The control functions are further dived into service control functions and resource control functions.

Resource control functions provide connectivity

Manuscript received April 21, 2009. This work was supported in part by the Research Project DO 02-135/15.12.2008, *Research on Cross Layer Optimization of Telecommunication Resource Allocation*, funded by Bulgarian Ministry of Education and Science.

control. The Policy and Charging Rule Function (PCRF) encompasses policy control decision and flow based charging control functionalities [4]. It is responsible for finding routes in the network that meet requirements for quality of service. The PCRF provides network control regarding the service data flow detection, gating, quality of service and flow based charging (except credit management) towards the PCEF. Media Resource Function Controller (MRFC) controls media resources. The Media Gateway Control Function (MGCF) controls the media gateway interfacing to circuited switched networks.

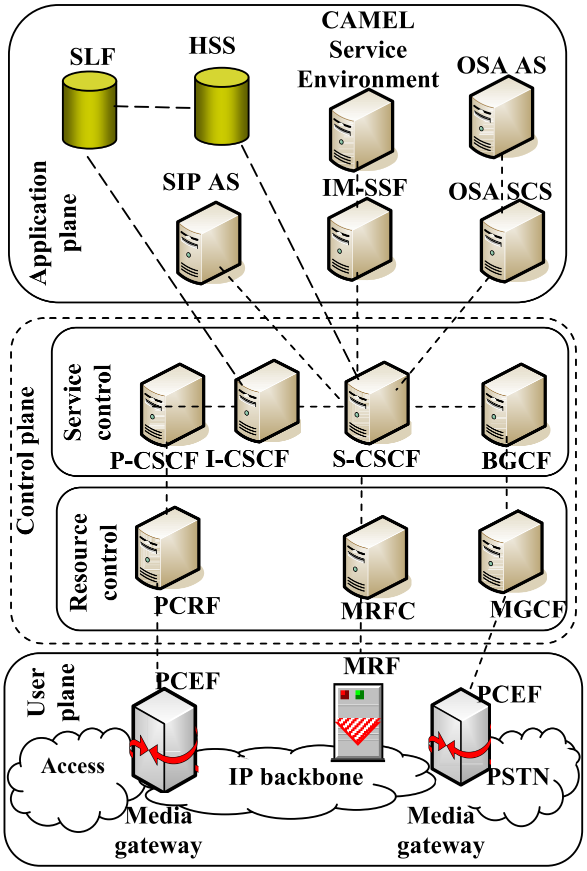


Fig.2 The IMS functional architecture

Service control functions are common functions for a number of services. The central role is played by Call Session Control Functions (CSCFs) used for multimedia session control and address translation function. In addition, the CSCFs manage service control, voice coder negotiation for audio communication, and authentication, authorization and accounting. The session control including management of dynamic inclusion/exclusion of elements in a session relies on Session Initiation Protocol (SIP) signalling [5]. The CSCFs are responsible for secure routing of the SIP messages, monitoring of the SIP sessions and communications with the PCRF to support media authorization. There are three kinds of CSCFs: Serving CSCF (S-CSCF), Proxy CSCF (P-CSCF) and Interrogating CSCF (I-CSCF). The P-CSCF is the first point of contact for the user equipment (user terminal) in the IMS. It is responsible for the security of SIP signalling between the user and the IMS, and SIP compression. The P-CSCF communicates with the PCRF to allocate resources for media flows. The I-CSCF plays a role of a SIP signalling gateway to external networks. It is responsible for assignment of an S-CSCF to the user during registration and for routing the incoming requests to an assigned S-CSCF or application server. The S-CSCF is the brain of the IMS and is always located at the home network. It performs session control and registration of user terminals. The Border Gateway Control Function (BGCF) is used in breakout scenarios to circuit switched networks.

The Application plane contains applications that extend network services using call control, messaging, user interaction, user location and flexible charging. The Application Server (AS) delivers value-added services. If the S-CSCF determines that the AS must be involved, it delegates the session control to that AS. The interface IMS Service Control (ISC) between the S-CSCF and the AS is based on SIP.

There are several types of application servers [6]. The SIP AS hosts applications that are able to influence the session control by receiving and emitting SIP signalling. The IP Multimedia Service Switching Function (IM-SSF) is an AS that allows services based on Customized Application for Mobile Enhanced service Logic (CAMEL) to be involved in session control. The Open Service Access (OSA) defines service architecture for third party application control on multimedia sessions through open interfaces. The OSA Application Programming Interfaces (APIs) define a standardized way for access to network functions (like call and session control, messaging, user interaction location etc.) and hide underlying network technology and protocol complexity from application developers. Network functions that can be accessed by external application through OSA APIs are defined as service capabilities. The OSA Service Capability Server (OSA SCS) interfaces between OSA applications and IMS service control. The OSA AS hosts third party applications that use network functions exposed through OSA APIs.

Home Subscriber Server (HSS) is an authentication server that stores authentication parameters applied for the users and user profiles that contain information about the media types that the users are authorized to use, and about the services that are to be applied to the users. The Subscription Locator Function (SLF) locates the HSS responsible for holding the user-related data for current user.

II. Quality of Service in IMS

A. *Quality of service mechanisms*

Resource management is the efficient and effective deployment for network resources when they are needed.

The resource management comprises different mechanisms to support the quality of service (QoS).

As to [7] Quality of Service is "the collective effect of service performance which determines the degree of satisfaction of a user of the service". The QoS is aimed to support the characteristics and properties of specific applications. Different applications may have quite different needs. For example, for e-commerce, the accuracy of the delivery is more important than overall delay or packet delay variation (i.e., jitter), while for IP telephony, jitter and delay are key and must be minimized.

To deliver service performance that determines the degree of user satisfaction of the service, an architectural framework for QoS support is defined. The QoS architectural framework is a set of generic network mechanisms for controlling the network service response to a service request, which can be specific to a network element, or for signalling between network elements, or for controlling and administering traffic across a network. As it is shown in Fig.3, the mechanisms are classified in three groups:

- Control mechanisms deal with the pathways through which user traffic travels. These mechanisms include admission control, QoS routing, and resource reservation. These mechanisms are realized by the PCRF.
- Data mechanisms deal with the user traffic directly. These mechanisms include buffer management, congestion avoidance, packet marking, queuing and scheduling, traffic classification, traffic policing and traffic shaping. These mechanisms are realized by the PCEF.
- Management mechanisms deal with the operation, administration and management aspects of the network. These mechanisms include Service Level Agreement (SLA), traffic restoration, metering and recording, and policy. These mechanisms are implemented in both PCRF and PCEF.

In IMS, service requirements are signalled at the Control plane and reflected on the underlying IP access and transport networks. Without interaction between User plane and Control plane the operator will not be able to provide the required QoS. The gateway contains a PCEF that has the capability of policing packet flow into the IP network, and restricting the set of IP destinations that may be reached according to a packet classifier. This service-based policy "gate" function has an external control interface that allows the gate to be selectively "opened" or "closed" on the basis of IP destination address and port. When open, the gate allows packets to pass through (to the destination specified in the classifier) and when closed, no packets are allowed to pass through. The control is performed by the PCRF which interacts with the P-CSCF. When the PCRF is implemented in a separate physical node, the interface between the PCRF and the P-CSCF is based on Diameter protocol [8].

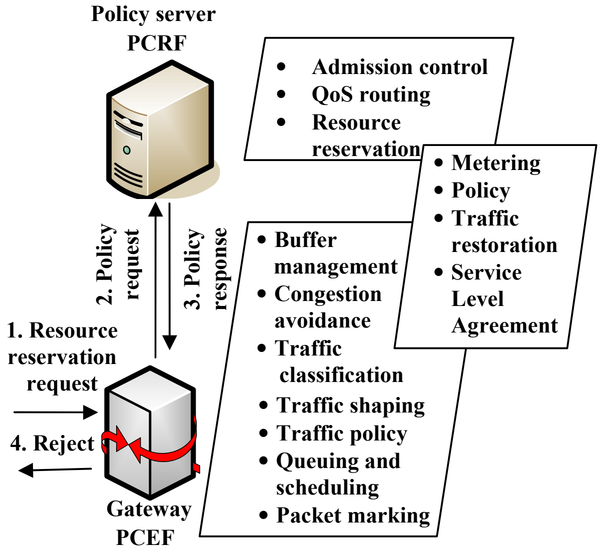


Fig.3 QoS mechanisms

The overall interaction between the network elements at the user plane and IMS control functions is called Service-Based Local Policy (SBLP) control [9]. There are eight interactions defined for Service-Based Local Policy:

- Authorization of QoS resources
- Resource reservation with Service-Based Local Policy
- Enabling media flows
- Disabling media flows
- Revoke authorization for QoS resources
- Indication of bearer release from the PCEF to the PCRF
- Authorization of QoS resource modification
- Indication of QoS resource modification from the PCEF to the PCRF.

B. Authorization of QoS Resources

The Session Description Protocol (SDP) is typically used to describe the desired session characteristics and the QoS requirements that must be met in order to successfully set up a session [10]. During SIP session establishment P-CSCF (PCRF) uses the SDP contained in the SIP signalling to calculate the proper authorization token. The token contains all the information needed to perform resource reservation. The P-CSCF includes the token in the response back to the user. The authorization is expressed in terms of the IP resources to be authorized and includes limits on IP packet flows, and may include restrictions on IP destination address and port. The principle of QoS resource authorization is illustrated in Fig.4.

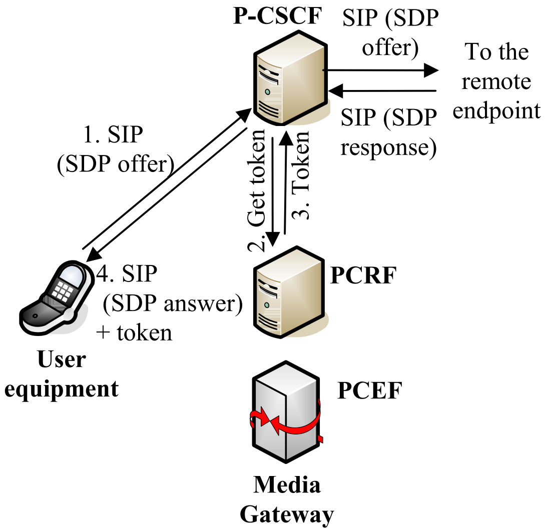


Fig.4 Authorization of QoS resources

C. *Reservation of QoS Resources*

Resource reservation is always initiated by the user equipment after successful authorization. The protocol used for resource reservation is referred to Resource reSerVation Protocol (RSVP) [11]. The user equipment includes in the RSVP message for resource reservation the authentication token granted. With request for QoS resource reservation, the PCEF in the gateway needs to assure that the requested resources match to the authorized resources. The PCEF forwards the token, together with the requested QoS parameters, to the PCRF. The PCRF checks if the corresponding requested QoS resources are within the limit of what was negotiated in the SDP exchange. The PCRF uses the token as the key to find the stored negotiated SDP. The principle of QoS resource reservation is illustrated in Fig.5.

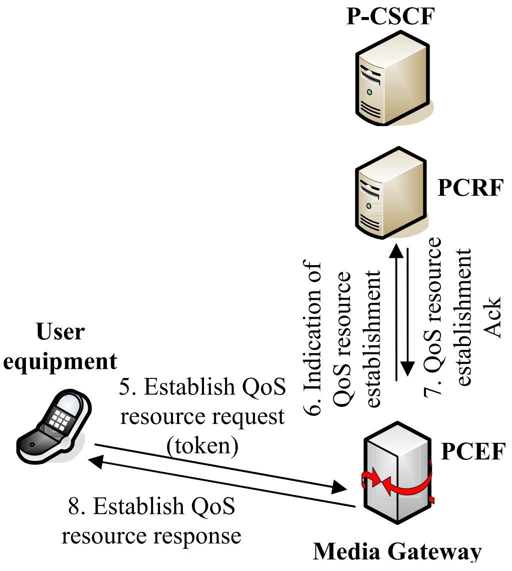

P-CSCF
PCRF
User equipment
6. Indication of QoS resource establishment
7. QoS resource establishment Ack
5. Establish QoS resource request (token)
8. Establish QoS resource response
PCEF
Media Gateway

Fig.5 Resource reservation of QoS resources

D. *Enabling media flows*

The PCRF makes policy decisions and provides an indication to the PCEF that the user is allowed to use the allocated QoS resources. The PCEF enforces the policy decisions and 'opens the door' for the user traffic.

E. *Disabling media flows*

The PCRF makes policy decisions and provides an indication to the PCEF about revoking the user's capacity to use the allocated QoS resources for per-session authorizations. The PCEF enforces the policy decisions and 'closes the door' blocking the user's media flows.

F. *Indication of QoS resource release*

Any release of QoS resources that were established based on authorization from the PCRF are reported to the PCRF by the PCEF. This indication is forwarded to the P-CSCF and may be used by the P-CSCF to initiate a session release towards the remote part. The principle of QoS resource release is illustrated in Fig.6.

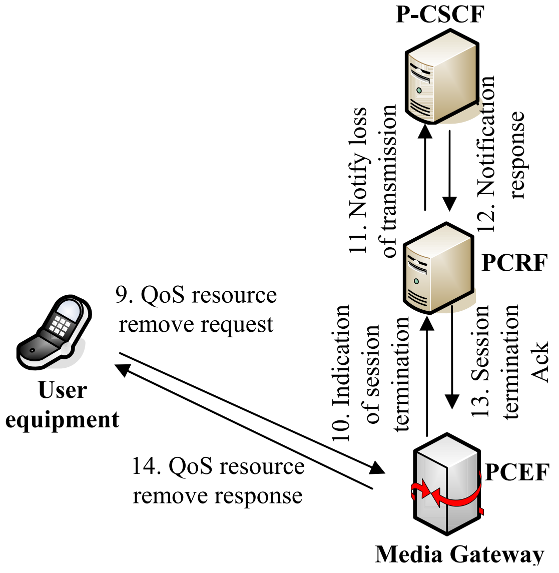

P-CSCF
11. Notify loss of transmission
12. Notification response
PCRF
9. QoS resource remove request
User equipment
10. Indication of session termination
13. Session termination Ack
14. QoS resource remove response
PCEF
Media Gateway

Fig.6 Release of QoS resources

G. *Revoke authorization for QoS resources*

At IP multimedia session release, the user equipment should deactivate the QoS resources used for the IP multimedia session. In various cases, such as loss of signal from the mobile, the user equipment is unable to perform this release itself. The PCRF provides indication to the PCEF when the resources previously authorized, and possibly allocated by the user equipment are to be released. The QoS resources are deactivated.

H. *Authorization of QoS resource modification*

When a QoS resource is modified by the user equipment, such that the requested QoS falls outside of the limits which were authorized, then the PCEF needs to verify the authorization of this QoS resource modification. If the PCEF does not have sufficient information to authorize the QoS resource modification request, the PCEF sends an authorization request to the PCRF. The PCRF authorizes the modified QoS resources based on the current session information.

It is also possible for the P-CSCF to send an update of the session information in case of a modification of a SIP session which results in an update of the authorization. The principle of QoS resource modification is illustrated in Fig.7.

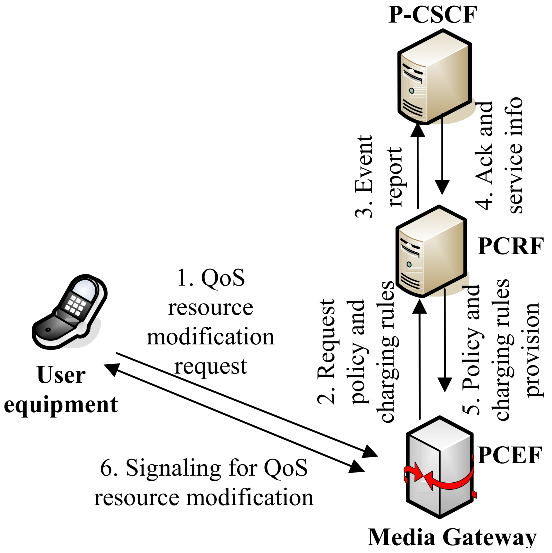

P-CSCF
3. Event report
4. Ack and service info
PCRF
2. Request policy and charging rules
5. Policy and charging rules provision
User equipment
1. QoS resource modification request
6. Signaling for QoS resource modification
PCEF
Media Gateway

Fig.7 Modification of QoS resources

I. *Indication of QoS resource modification*

When a QoS resource is modified such that the maximum bit rate (downlink and uplink) is downgraded to 0 bit/s or changed from 0 kbps to a value that falls within the limits that were authorized, then the PCEF has to report this to the PCRF. This indication is forwarded to the P-CSCF. The P-CSCF uses this information to initiate a session release towards the remote endpoint.

J. *Event and information distribution*

The S-CSCF and Application Servers (SIP-AS, IM-SSF, OSA-SCS) must be able to send service information messages to endpoints. This is done using a SIP Request/Response information exchange containing the service information and/or a list of addresses pointing to the location of information represented in other media formats. The stimulus for initiating the service event related information message may come from e.g. a service logic residing in an AS.

In addition, the endpoints are also able to send information to each other. This information is delivered using SIP based messages. The corresponding SIP messages are forwarded along the IMS SIP signalling path. This includes the S-CSCF but may also include SIP Application Servers.

The service event related information exchange may either take place in the context of a session, or independently outside the context of any existing session.

The principle of QoS event and information distribution is shown in Fig.8.

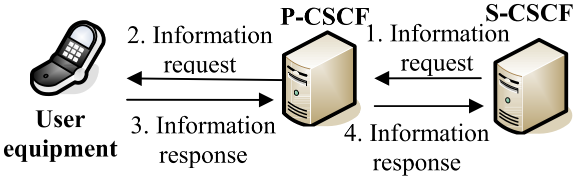


Fig.8 Distribution of QoS events and information

An Application Server offering value-added services including QoS management applications resides either in the user's home network or at a third party location. The third party could be a network or simply a stand-alone AS. For resource control purposes, some applications may interact with the PCRF, while others rely on the S-CSCF providing the basic session over which the value-added application is built.

To present the way in which applications can manage the QoS, it is necessary to have a notion of service control.

III. Service Control

A. *Service Triggering*

Applications that are hosted by and execute on an application server may be invoked by a request from the S-CSCF or may be initiated by another mechanism. Applications may issue session control signalling via the S-CSCF and may therefore influence the multimedia session. Information about the applications that are to be triggered on behalf of the user (i.e., about the application servers that will need to be contacted whenever the user issues a request) is stored in HSS. The application might be invoked for the originating part and for the terminating part as shown in Fig.9.

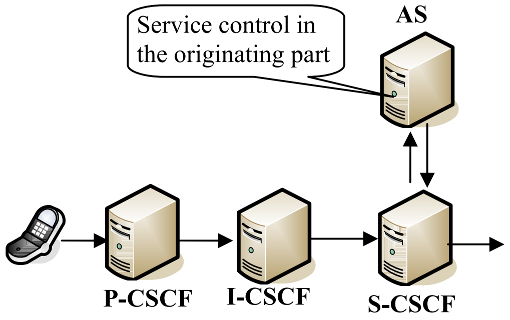


Fig.9 (a) Application control in the originating part

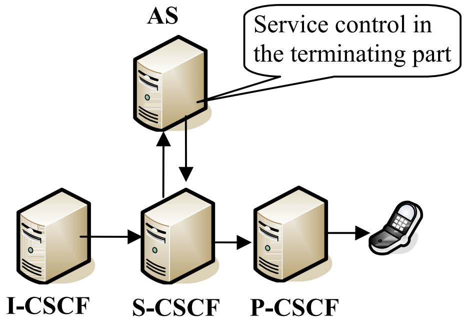


Fig.9 (b) Application control in the terminating part

Initial filter criteria (iFC) describe the way in which the user can access the multimedia services. The iFC contain information about service triggering and describe when an incoming SIP message is further routed to a specific AS. They are downloaded to the S-CSCF upon user registration as shown in Fig.10.

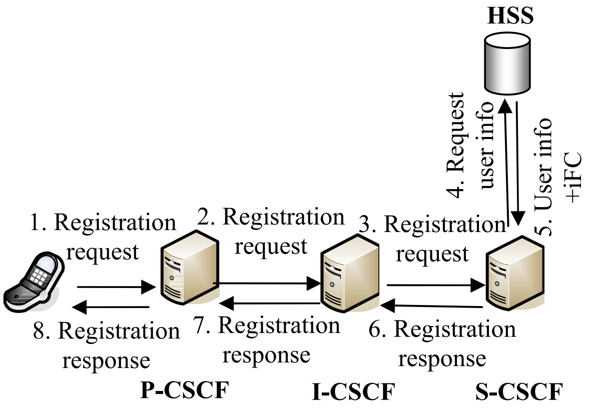


Fig.10 Downloading iFC into the S-CSCF on user registration

On receiving a SIP request, the S-CSCF checks the conditions for service triggering, i.e. determines if some of the iFC are met. If it is so, the S-CSCF delegates the service control to the appropriate AS. The principle of service triggering is shown in Fig.11.

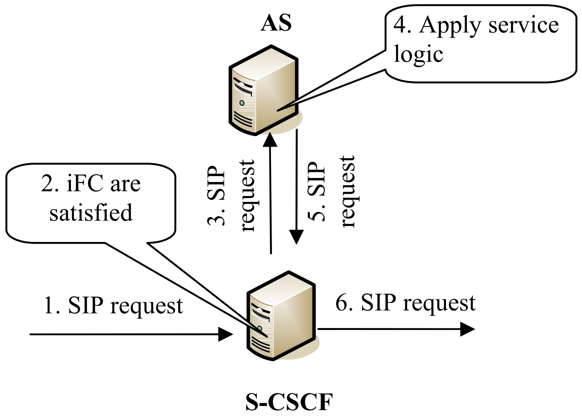
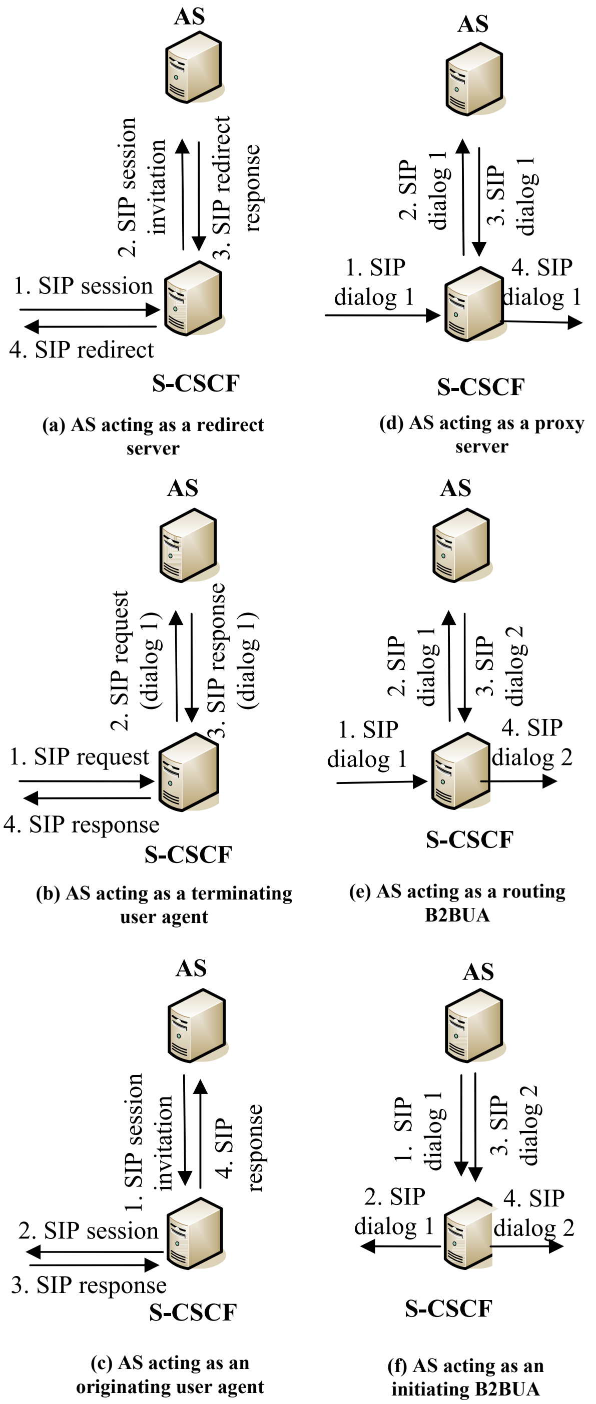


Fig.11 Service triggering

In processing the SIP request the AS can play different roles. The AS roles are illustrated in Fig.12.



(a) AS acting as a redirect server

(d) AS acting as a proxy server

(b) AS acting as a terminating user agent

(e) AS acting as a routing B2BUA

(c) AS acting as an originating user agent

(f) AS acting as an initiating B2BUA

Fig.12 Application Server roles

In case (a) of acting as a redirect server, the AS receives the incoming SIP request and uses the service information to send a redirection response. In case (b) of acting as a terminating user agent, the AS can establish a session with the originating user agent. In case (c) of acting as an originating user agent, the AS generates a SIP request and sends it to the S-CSCF which then proxies it towards destination. Case (d) occurs when the AS acting as a SIP proxy receives incoming SIP request and proxies it back to the S-CSCF which then proxies it towards the destination. Case (e) shows an AS acting as a routing Back-to-Back User Agent (B2BUA) which performs third party call control. In this case the AS receives the incoming SIP request, generates a new SIP request and sends it to the S-CSCF which in turn proxies it towards the destination. Case (f) shows another type of third party application control by an AS. In this case the AS acting as an initiating B2BUA initiate two new requests within different SIP dialogs. These requests are proxied through the S-CSCF which in turn forwards them to their destinations.

Usually a native SIP AS offers purely SIP-based services. An operator can also offer access to services based on the Customized Applications for Mobile network Enhanced Logic (CAMEL) Service Environment and the Open Service Access (OSA) for its IMS subscribers. The IM-SSF AS provides access for IMS users to existing Intelligent Network services. The OSA service capability servers offer the OSA interface to the OSA Application Server running third party applications. In comparison to CAMEL-based services which are restricted to the operator domain, OSA opens network interfaces for external applications and allows secure access to functions such as call and session control, location management, charging, messaging and QoS management.

In the next section we explain in brief basic concepts of the open service access and then focus on OSA service capabilities for resource management.

IV. Open Access to Network Functions

A. Open Service Access and Parlay Overview

Open Service Access (OSA) is defined as a service architecture for delivering value-added services in third generation mobile networks [12]. It adopts the approach of the classical Intelligent Network for service assembling out of components. But while the Intelligent Network concept fits well to circuit-switched networks, the OSA provides underlying network independence.

In OSA, the functions provided by the network are defined as service capabilities servers (SCS). The elementary SCS functions are grouped into Service Capability Features (SCF). A SCF is a unit of functionality that can be used as a reusable building block for services. Examples of features are call and session control, user interaction, messaging, accessing user status and user location and so on. Fig.13 gives an overview of OSA.

To make easier service creation, OSA defines object-oriented application programming interfaces (APIs) for each SCF. The APIs abstract the details of the underlying network service capabilities and data. They are specified in an implementation-independent way in a form of Interface Definition Language (IDL) definitions and Unified Modelling Language (UML) descriptions [12]. The APIs are implementable in a distributed computing environment. The usage of API for service creation hides for developers the complexity of the network control protocols and encapsulates network implementation.

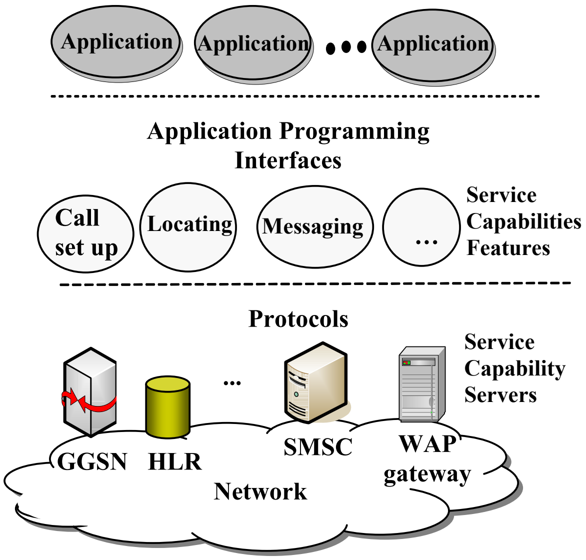


Fig.13 The concept of Open Service Access

The OSA API definition is strongly influenced by Parlay programming interfaces. The concept of Parlay is to open network interfaces for third party software developers (other than network operator and service provider). The Parlay interfaces also allow access to network functions, such as call and session control, messaging, charging, QoS management. Network access to third party applications is secured. Before using network functions third party applications are subject to authentication and authorization. To avoid repudiation applications are required to digitally sign an on-line agreement for the use of certain features.

Because of their similarity the Parlay and OSA interface specifications have been aligned.

OSA and Parlay consists of 13 interface groups, listed in Table I. The Framework is a special interface with common functions for authentication, discovery and manageability required to enable services to work together in a coherent manner. The other interfaces are service interfaces that allow applications to control network resources.

The OSA APIs are split into three types of interface classes as shown in Fig.14. Interface classes between the applications and the framework provide applications with basic mechanisms enabling applications to make use of the service capabilities in the network. Interface classes between applications and SCFs allow application to access to network functions. Interface classes between the framework and the SCFs provide the mechanisms necessary for a multi-vendor environment. Network side interfaces' names are prefixed with "Ip" and application side interfaces' names are prefixed with "IpApp".

TABLE I
PARLAY/OSA INTERFACES

Interface	Short description
Framework	Authentication, authorization, service discovery, service subscription, integrity management
Call control	Setup and control of multiparty multimedia calls and conferences, notification of call and connection-related events
User interaction	Playing announcements, retrieving user input, sending short messages
Mobility	Provisioning information for user status and user location
Terminal Capabilities	Getting capabilities of end user terminals
Data session control	Setup and control of packet data sessions
Connectivity management	Negotiation and management of QoS in IP networks
Account management	Creating, modifying and deleting subscriber accounts
Charging	Reservation and charging of units of volume or money against subscriber accounts, split charging
Policy management	Defining policy information including service level agreements, evaluating policies and subscription for and notification of policy events
Presence and availability management	Managing, retrieving and publishing user-related information including identities, communication capabilities, content delivery capabilities, state information, presence and availability of entities for different contexts and communication methods
Multimedia messaging	Sending, storing and receiving multimedia messages, manipulating mailboxes and mail directories
Service brokering	Registering the application interest in particular traffic as part of service interactions

Each OSA interface is defined as a set of object types (classes). A class defines the methods that can be called on the object and their parameters. The method definition includes also the method type and exceptions. The method type defines the type of the result returned. The exceptions define errors that may arise during the method execution.

Two OSA SCFs are defined for the purpose of resource management in IMS:

- OSA Connectivity Manager API
- OSA Policy Management API.

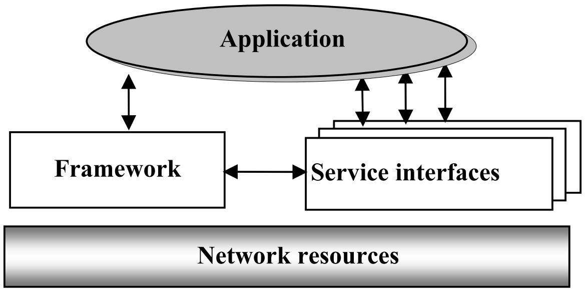


Fig.14 OSA interface types

B. OSA Connectivity Management

The Connectivity Management is a set of functions that provide configuration and control of both the attributes of IP connectivity and policies governing IP connectivity, within and between IP domains. Such attributes include QoS, security, and routing policy.

The "OSA Connectivity Manager" SCF is defined to establish QoS parameters for an enterprise network traffic travelling through a provider network. Assuming that the underlying packet network can be configured as a virtual private network (VPN), the Connectivity Manager interfaces provide methods that allow management applications to configure inter-site virtual connections.

The "Connectivity Manager SCF" can be used by a VPN client (enterprise operator subscribed for VPN services) that has entered a relationship with a VPN provider (network operator) to set up a provisioned QoS. Connectivity Manager includes API between VPN client and VPN provider to establish QoS parameters for VPN packets passing through the provider network.

The API requires any specific QoS method to be used neither in the VPN network nor in the operator network. To deliver QoS between networks the differentiated services approach is used which is based on giving preferential treatment to some packets over others in the edge routers. Each packet arriving from the VPN client network into the VPN provider network is marked with a tag called DSCP (differentiated services code point). Only marked packets can enjoy the QoS service provisioned in the VPN provider network.

The VPN client may be an enterprise operator that owns a number of enterprise sites connected via virtual private network provided by a VPN provider. The VPN provider is available at a number of sites by service access points for the VPN client. An application using "Connectivity Manager" SCF is hosted at the VPN client domain. The telecom operator gives the VPN provider access to the "Connectivity Manager" SCF. The access through an OSA SCS is subject to the safeguards provided by the Framework. An imaginary VPN configuration is shown in Fig.15.

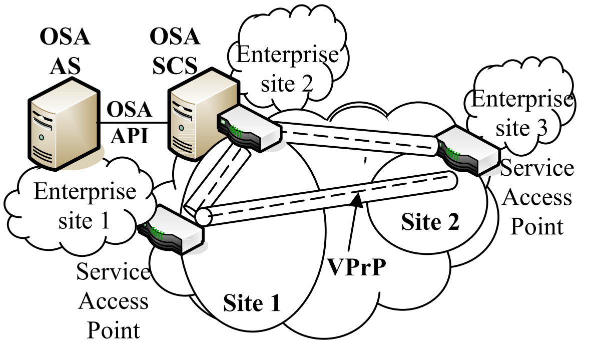


Fig.15 An imaginary Virtual Private Network of an enterprise operator

The VPN provider offers configuration service to the VPN client. Using the "Connectivity Manager" API the VPN client can create virtual provisioned pipes (VPrP) in the VPN provider network to carry the enterprise traffic and support it with pre-specified QoS. The VPrP defines QoS parameters for traffic flowing through the provider network between two specified enterprise endpoints. The VPN provider offers a set of templates that are used by the VPN client to specify a VPrP. For instance, the provider may offer templates for video conferencing, audio conferencing, Gold Service, Silver Service, etc. Using these templates the VPN client can select and provision a VPrP with specific QoS attributes. Elements that can be specified for a VPrP include attributes such as packet delay and packet loss, and traffic characteristics such as maximum rate and burst rate. The collection of all the VPrPs, provisioned within the enterprise VPN, constitutes the Virtual Provisioned Network (VPrN).

Fig.16 shows the UML class diagram of the "Connectivity Manager" interfaces. The figure shows the aggregation association between classes with the multiplicity notations near the end of the associations. The Connectivity Manager interface is the entry point to this service. From this interface the client application can get reference to the VPN client network interface and to the QoS menu interface. The QoS menu interface provides a list of templates, each of which specifies the QoS service parameters that are offered by the VPN provider. The service is composed of components that are associated with a provisioned QoS. The client application can use the template interface to specify the service parameters that are offered by the VPN provider, and also, to store the parameters that the VPN client selects temporarily. The VPN client network interface is associated with two components: enterprise sites, and the VPrN that has been already provisioned in the provider network. The Virtual Provisioned Network interface contains references to all the VPrPs already established. The client application can use the QoS Menu to get references to all the QoS templates offered by the provider. Once the VPN client selects the QoS parameters provided in the QoS template, and submits the request to create a new VPrP, the VPN provider validates the information submitted and if the request is approved, the new VPrP is activated**.**

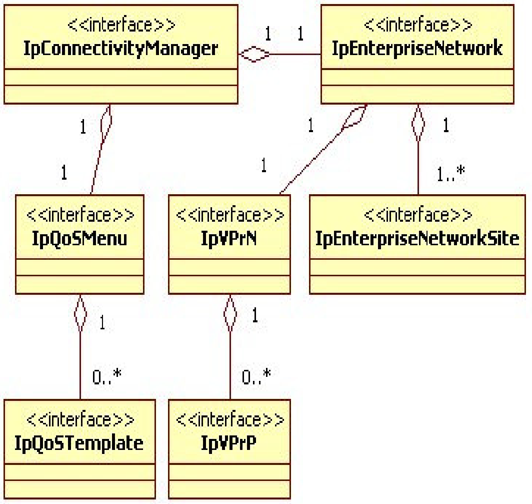


Fig.16 OSA Connectivity Manager interfaces

After successful authentication and authorization the enterprise OSA application may use the methods supported by the IpConnectivityManager interface to get the handle to the menu of QoS services offered by the VPN provider, and to get a handle to the enterprise network interface that holds information about current services that the provider network delivers to the enterprise network.

The IpQoSMenu interface holds the QoS menu offered by the provider. Each QoS service offered (e.g. Gold, Silver) is specified in a separate template. When the VPN client asks for a specific template from the list of templates, a temporary template interface is created. This temporary template interface holds all the parameters (e.g. all the Gold parameters) and their default values offered by the provider for this template.

The IpQoSTemplate interface provides access to a specific QoS template, such as Gold, offered by the provider. This interface provides getters to discover the QoS service details, and setters to set the requested values for a new VPrP.

The VPN client can create a new Virtual Provisioned Pipe (VPrP) in an existing VPN with the IpVPrN interface. Each such pipe is associated with QoS parameters identified by a specific DiffServ Codepoint. A packet that arrives at a service access point with a specific Codepoint, is "directed" to the VPrP that supports the QoS parameters provisioned for this pipe. The VPN client can create new VPrPs and delete existing VPrP using the IpVPrN interface. This interface provides also methods to get the list of already provisioned VPrPs, and a handle to a specific VPrP interface that holds information for this VPrP.

Fig.17 illustrates the sequence in which VPN client selects service components and creates a new VPrP. In the figure, the client application collects the information required to select a service, then selects service parameters, and finally submits it to the Connectivity manager.

The IpEnterpriseNetwork interface stores enterprise network information maintained by the provider as it relates to the VPN service and the virtual provisioned network service that the VPN client had already established with the provider network. The VPN client can only retrieve information regarding an existing VPrN, list the sites connected to the VPN, and get the handle to a specific site interface that stores information about the site.

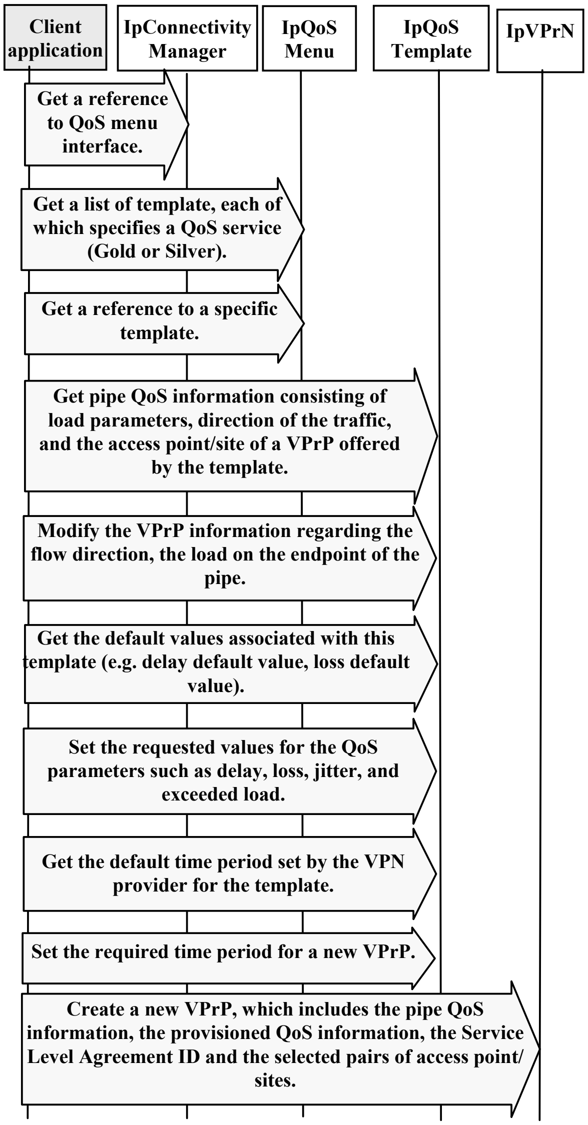

Client application
IpConnectivity Manager
IpQoS Menu
IpQoS Template
IpVPrN
Get a reference to QoS menu interface.
Get a list of template, each of which specifies a QoS service (Gold or Silver).
Get a reference to a specific template.
Get pipe QoS information consisting of load parameters, direction of the traffic, and the access point/site of a VPrP offered by the template.
Modify the VPrP information regarding the flow direction, the load on the endpoint of the pipe.
Get the default values associated with this template (e.g. delay default value, loss default value).
Set the requested values for the QoS parameters such as delay, loss, jitter, and exceeded load.
Get the default time period set by the VPN provider for the template.
Set the required time period for a new VPrP.
Create a new VPrP, which includes the pipe QoS information, the provisioned QoS information, the Service Level Agreement ID and the selected pairs of access point/ sites.

Fig.17 The Application creates a new virtual provisioned pipe

Fig.18 illustrates the way in which a VPN client browses a VPrP. Using the IpVPrP interface the client application browses and collects information regarding existing VPrP, including all the QoS parameters that have been set for this pipe.

The IpVPrP interface provides information on a VPrP whose status can be in one of the following states:

- *Active*: a previously established VPrP, which indicates that a previous request to create the VPrP was granted by the provider. Packets that belong to this VPrP and meet the validity time requirements are admitted to the VPrN.
- *Pending*: a request to create a new VPrP is still pending response from the provider, indicating that the provider is still processing the request to create a new VPrP. Packets that belong to this VPrP are not admitted to the VPrN.
- *Disallowed*: a request to create a new VPrP was denied. A description parameter may include the reason for the denial. This is a disallowed VPrP and packets that belong to this VPrP are not admitted to the VPrN.

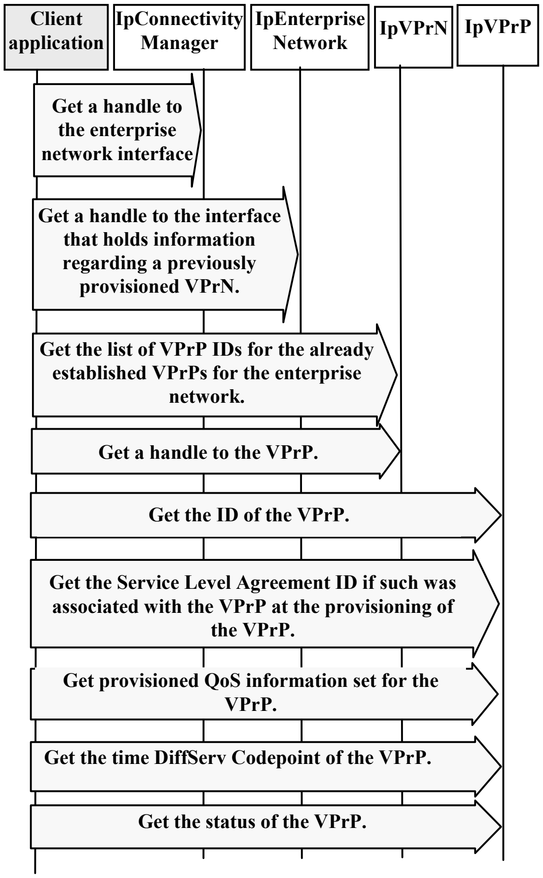

Client application
IpConnectivity Manager
IpEnterprise Network
IpVPrN
IpVPrP
Get a handle to the enterprise network interface
Get a handle to the interface that holds information regarding a previously provisioned VPrN.
Get the list of VPrP IDs for the already established VPrPs for the enterprise network.
Get a handle to the VPrP.
Get the ID of the VPrP.
Get the Service Level Agreement ID if such was associated with the VPrP at the provisioning of the VPrP.
Get provisioned QoS information set for the VPrP.
Get the time DiffServ Codepoint of the VPrP.
Get the status of the VPrP.

Fig.18 The Application browses a virtual provisioned pipe

The IpEnterpriseNetworkSite stores site information of the VPN client network. This information is maintained by the VPN provider.

Fig.19 shows the way in which a VPN client browses service access points and sites. The client application browses service access points and sites to retrieve information for a site and its service access points.

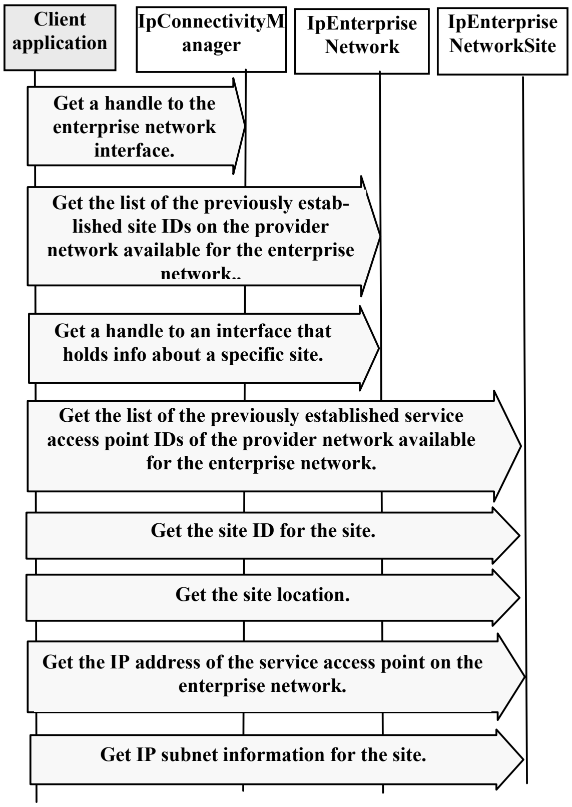

Client application
IpConnectivityManager
IpEnterprise Network
IpEnterprise NetworkSite
Get a handle to the enterprise network interface.
Get the list of the previously established site IDs on the provider network available for the enterprise network..
Get a handle to an interface that holds info about a specific site.
Get the list of the previously established service access point IDs of the provider network available for the enterprise network.
Get the site ID for the site.
Get the site location.
Get the IP address of the service access point on the enterprise network.
Get IP subnet information for the site.

Fig.19 The Application browses service access points and sites

The OSA "Connectivity Manager" SCF is defined in [13].

C. *OSA Policy Management*

The "Policy Management" SCF is defined to support policy-enabled services.

Policy is an ordered combination of policy rules that define how to administer, manage, and control access to resources. Policy rule is a combination of conditions and actions to be performed if the condition is true. Policy evaluation is the process of evaluating the policy conditions and executing the associated policy actions up to the point that the end of the policy is reached. The repository is meant to hold unattached conditions and actions. The network operator can populate the repository with the conditions and actions that it can support.

Fig.20 shows the OSA Policy Management architecture in IMS environment. The PCRF, PCEF and Policy repository form network policy engine.

The UML class diagram of "Policy Management" interfaces is shown in Fig.21. The figure presents the interface inheritance hierarchy. Some of the interfaces are omitted for simplicity.

The OSA "Policy Management" interfaces allow policies to be provisioned and compliance of service usage with policies to be evaluated. Policy-based management provides a way to allocate network resources, primarily network bandwidth, quality of service (QoS), and security (such as firewalls), according to defined business policies.

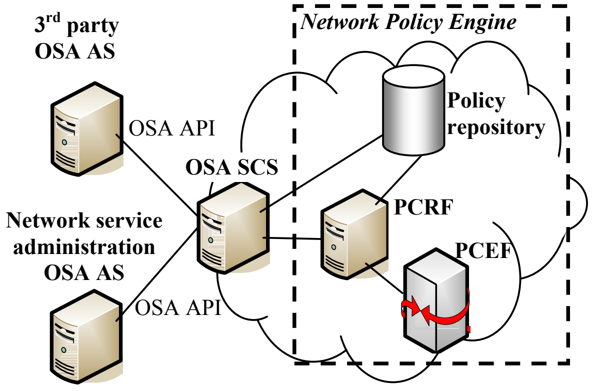


Fig.20 Policy management architecture

Client (3rd party) applications can use the Policy Management API to create, update or view policy information for any policy enabled service. It is possible for an application to subscribe to policy events, to request evaluation of policies and to request the generation of policy events.

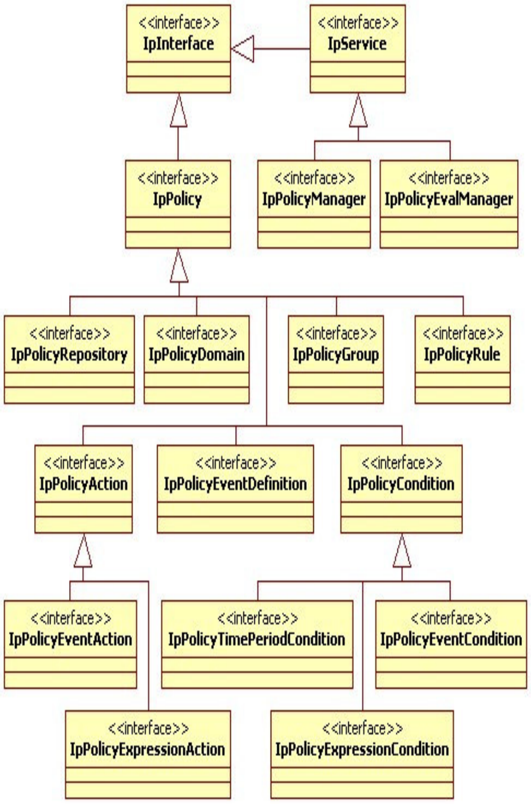

<<interface>> IpInterface
<<interface>> IpService
<<interface>> IpPolicy
<<interface>> IpPolicyManager
<<interface>> IpPolicyEvalManager
<<interface>> IpPolicyRepository
<<interface>> IpPolicyDomain
<<interface>> IpPolicyGroup
<<interface>> IpPolicyRule
<<interface>> IpPolicyAction
<<interface>> IpPolicyEventDefinition
<<interface>> IpPolicyCondition
<<interface>> IpPolicyEventAction
<<interface>> IpPolicyTimePeriodCondition
<<interface>> IpPolicyEventCondition
<<interface>> IpPolicyExpressionAction
<<interface>> IpPolicyExpressionCondition

Fig.21 OSA Policy Management interfaces

The OSA "Policy Management" SCF comprises of the following interfaces classes:

- Policy Management Provisioning Service interfaces used to define policy information, including policy rules, policy events, etc., and to update and view this information.

- Policy Management Evaluation interfaces used to request evaluation of policies and for subscription and notification to policy events.

The client applications participating in Policy Management use the IpPolicyManager to reference a policy domain of interest, create a new policy domain or remove an existing one. Client applications also can reference a policy repository, to create a new policy repository or remove an existing one.

The IpPolicy is the base interface from which are derived all of the Policy interfaces (except IpPolicy-Manager and IpPolicyEvalManager). This interface documents attributes for describing a policy-related instances.

The IpPolicyDomain interface allows aggregation of Policy Domains, Policy Groups, Policy Rules, or Policy Event Definitions in a single container. The Policy Domains and their nesting capabilities are shown in Fig.22. For an example, the Policy domain for resource management can nest other Policy domains that provide specialized rules regarding to QoS management.

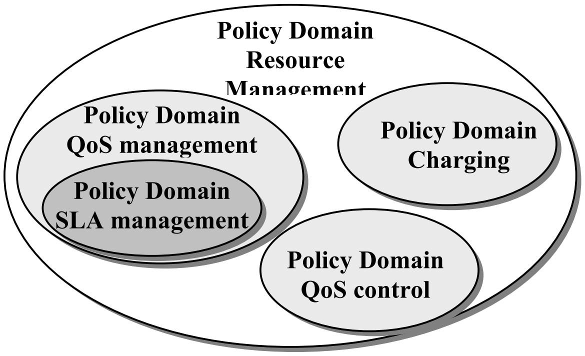


Fig.22 Policy domains

The IpPolicyGroup interface allows aggregation of Policy Rules or other Policy Groups in a single container. The Policy Groups and their nesting capabilities are shown in Fig.23. For an example, the Policy Group SLA is used to define the policy based on the content of the Service Level Agreement (SLA) templates. It can nests Policy Groups for QoS parameters regarding the technology part of the SLA template.

The IpPolicyRepository interface represents a container for reusable policy-related information. The Policy Repository containing Policy Conditions and Policy Actions can be used in definition of one or more Policy Rules.

The IpPolicyRule represents the semantics of conditions and actions associated with a policy. A policy rule is define in a form of “if Condition then Action”. The conditions and actions associated with a policy rule are modelled respectively with IpPolicyCondition and IpPolicyAction interfaces. A policy rule may also be associated with one or more policy time periods indicating when the policy rule is active or inactive.

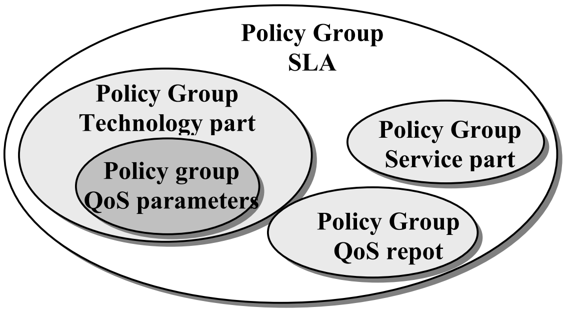


Fig.23 Policy groups

The policy time periods are modelled by the IpPolicyTimePeriodCondition interface. For example, a policy rule may define actions for traffic shaping in case the user has exceeded the negotiated in SLA maximum rate for more than an hour. IpPolicyExpressionCondition interface is used to generate a Policy condition regarded to a specified event. The IpPolicyExpressionAction interface is used to evaluate an expression.

The example shown in Fig.24 may be used to implement Service-based local policy control, which is a way of managing the access network through policies. It allows policy control over IP bearer resources.

As described in section 2, it is important for an operator to correlate the QoS requested at the session layer (through session control signalling, such as SIP) with the actual QoS provided at the bearer level (initiation of QoS resources). The binding between the media components specified at the session layer and the corresponding QoS resources maintained at the edge router, is ensured by using an authorization token. One authorization token is assigned per IMS (SIP) session; each media component (e.g. video or audio) in a SIP session is identified by a sequence number. The token provided during the authorization of the media session and sent in the QoS resource reservation request is used as the mechanism to enable the edge router to contact the PCRF that generated the token. First, the PCRF verifies that the QoS resource activation request corresponds to an ongoing session. Second, it verifies that the requested bearer QoS corresponds to media resource information authorized by the P-CSCF.

Fig.24 shows the sequence in which the operator can define a policy domain regarded to Admission Control procedures, a policy group with policy rule for authorization of QoS resources.

The IpPolicyEventDefinition interface specifies the required and optional attributes of events that can be subscribed to, specified as conditions, and generated by clients or actions. A Policy Condition that is satisfied when the specified event with the matching attributes is generated is modelled by the IpPolicyEventCondition interface. The IpPolicyEventAction interface represents specified events.

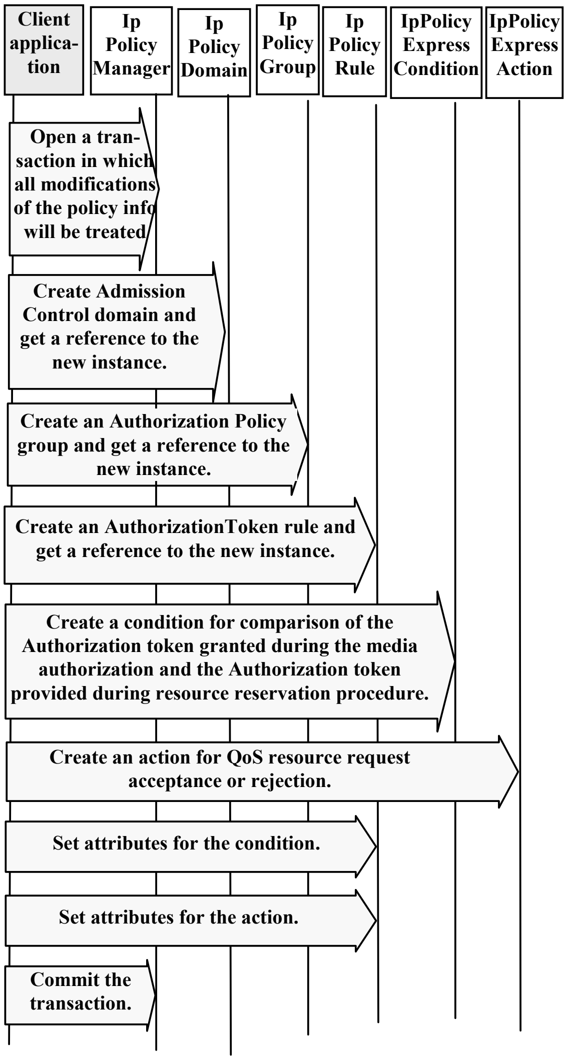

Client applica- tion
Ip Policy Manager
Ip Policy Domain
Ip Policy Group
Ip Policy Rule
IpPolicy Express Condition
IpPolicy Express Action
Open a tran- saction in which all modifications of the policy info will be treated
Create Admission Control domain and get a reference to the new instance.
Create an Authorization Policy group and get a reference to the new instance.
Create an AuthorizationToken rule and get a reference to the new instance.
Create a condition for comparison of the Authorization token granted during the media authorization and the Authorization token provided during resource reservation procedure.
Create an action for QoS resource request acceptance or rejection.
Set attributes for the condition.
Set attributes for the action.
Commit the transaction.

Fig.24 The OSA application creates a policy domain, policy group and a policy rule

A client application can use the IpPolicyEvalManager interface to evaluate policy rules, to subscribe to and receive notifications of policy events and to generate events.

The IpAppPolicyDomain interface is supported by the client application and returns values.

Fig.25 shows how policy events are used. For example, a client application may define an event concerning unsuccessful resource reservation based on comparison of requested QoS resources and the authorized session QoS resources.

Fig.26 illustrates how a client subscribes to a policy event and receives notification when the event is triggered.

Assuming that the policy event has been defined, the event is triggered when the action part of a rule fires. This may happen when for example the Authorization token provided during the QoS resource reservation procedure does not match to the Authorization token granted during the media authorization of session QoS resources causing the condition of a policy rule to be satisfied thus resulting in the action part to be executed.

The OSA "Policy Management" SCF is defined in [14].

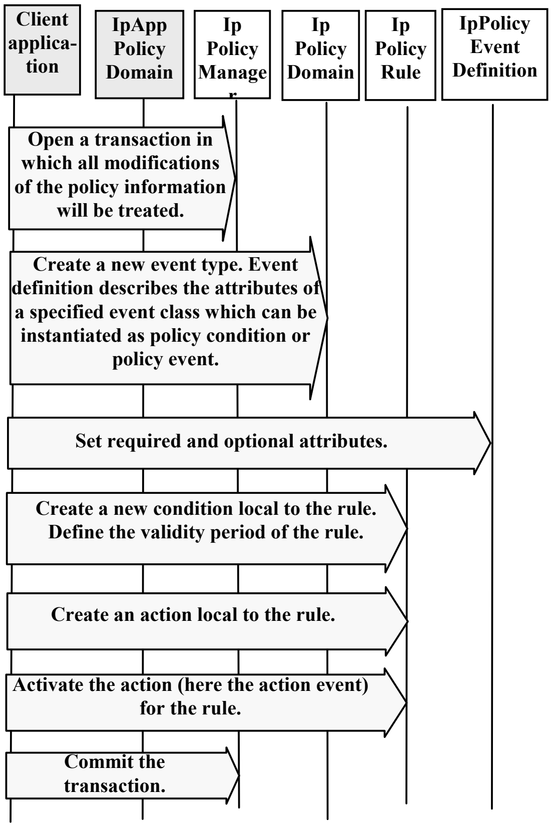

Client applica- tion
IpApp Policy Domain
Ip Policy Manage r
Ip Policy Domain
Ip Policy Rule
IpPolicy Event Definition
Open a transaction in which all modifications of the policy information will be treated.
Create a new event type. Event definition describes the attributes of a specified event class which can be instantiated as policy condition or policy event.
Set required and optional attributes.
Create a new condition local to the rule. Define the validity period of the rule.
Create an action local to the rule.
Activate the action (here the action event) for the rule.
Commit the transaction.

Fig.25 The OSA application uses a template to define allowable events

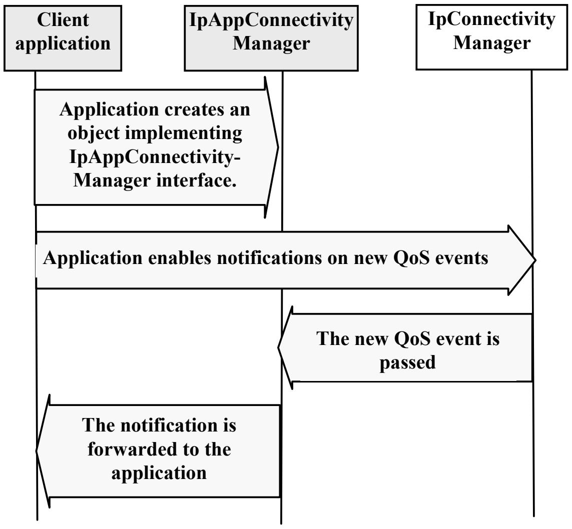

Client application
IpAppConnectivity Manager
IpConnectivity Manager
Application creates an object implementing IpAppConnectivity- Manager interface.
Application enables notifications on new QoS events
The new QoS event is passed
The notification is forwarded to the application

Fig.26 The OSA application registers for and receives notification of a policy event

V. Parlay X Web Services

A. Parlay X Overview

The Parlay/OSA APIs expose telecommunication functions in a network technology and programming language neutral way. Covering common programmability aspects of (converged) mobile, fixed, and managed packet networks, the APIs provide a medium level of abstraction of the network capabilities. They provide an abstraction from different specific protocols, but the abstraction level of Parlay/OSA APIs is not judged to be oriented to traditional IT-developers and this could affect usability. To open the accessibility of the network capabilities to a much wider audience Parlay X provides a set of high level interfaces that are oriented towards the skill levels and telecom knowledge levels of web developers.

The Parlay X is the name of the interface for accessing Parlay/OSA APIs using Web Services. The Web Services architecture realizes an interoperable network of services focused on service reuse. In addition to being a Web Services interface, the Parlay X interface is much simplified presentation of Parlay/OSA APIs.

Web Services operations and access are described by the Web Services Definition Language (WSDL). The Web Service provider publishes Web Services through a registry, making those Web Services available for discovery. Web Services applications use the Simple Object Access Protocol (SOAP) to exchange information.

Fig.27 shows how Parlay X Web Services may be deployed in IMS environment.

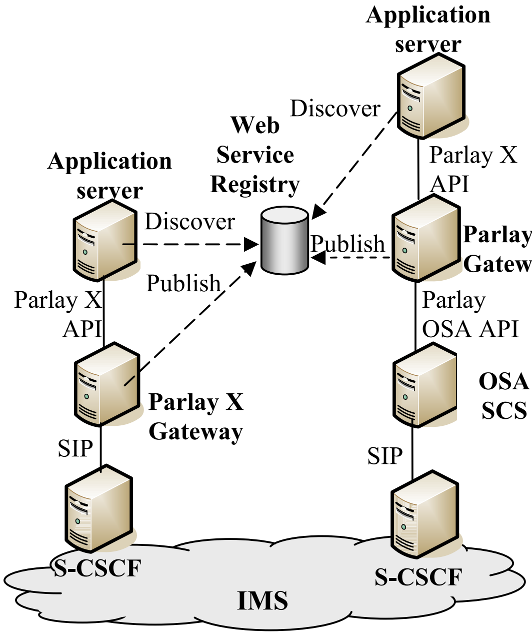


Fig.27 Parlay X Web Services deployment in IMS

The Application server (AS) hosts Parlay X applications. The information published to the Web Services Registry provides applications with the connection information required to connect with the Parlay X Web Services Gateway. The applications access Web services through the Parlay X Gateway and the implementation behind the gateway is not visible for them. The Parlay X Gateway may be attached directly to the network element (S-CSCF) or to the OSA SCS. In the first case, the Parlay X Gateway plays a role of SIP AS and 'talks' SIP at the side of the network. In the other case, the Parlay X Gateway attaches to the OSA SCS through OSA interfaces.

The list of presently available Parlay X Web services is shown in Table II.

Up to now, two Parlay X Web services that can be used for resource management purposes in IMS are defined:

- "Application-driven Quality of Service" Parlay X Web Service
- "Policy" Parlay X Web Service.

B. Application-driven quality of service Parlay X Web Service

Using the "Application Driven QoS" Parlay X Web service applications can dynamically change the QoS available on end user network connections. Configurable service attributes are upstream bandwidth rate, downstream bandwidth rate and other QoS properties specified by the service provider. Changes in QoS may be applied on either for a defined period of time, or each time a user connects to the network. Application-driven QoS Web Service enables applications to register with the service for notifications about network events that affect QoS temporary configured on the end-user's connection. On such event occurrence the service notifies the applications.

The Application Driven QoS Web Service provides three interfaces.

The ApplicationQoS interface supports methods that allow the Application to apply a new QoS feature on end user connections, to modify active QoS features on end user connections or to release temporary QoS currently active on end used connection. Using the ApplicationQoS interface the application can retrieve the status of end user connections. The ApplicationQoSNotificationManager interface is used by the Application to manage the registration for notifications. The ApplicationQoS-Notification interface provides method for notifying the Application about the impact of certain events on QoS features that were active on the end user connection where these events occurred.

Fig.28 shows an example of where the Application applies a temporary QoS feature to an end user connection, then modifies the active temporary QoS feature and at last removes the active QoS feature. This scenario might be applied for an end user with contracted 1 Mbps DSL service wishing to stream a piece of video content. The video stream lasts two hours and a temporary bandwidth upgrade is required to support streaming.

TABLE II
PARLAY X WEB SERVICES

Parlay X Web Service	Short description
Third party call	Call initiation from one caller to another by third party
Network initiated third party call	Call control on calls in the network by third party
Short Message Service	Submitting and receiving text messages
Multimedia message	Submitting and receiving multimedia messages
Payment	Initiation of payment sessions according to different charging methods
Account management	Checking account status, such as account balance, account credit expiration, etc.
Terminal status	Getting terminal status information
Terminal location	Getting location information
Call handling	Call control by third party
Audio call	Supporting a call with associated audio content
Multimedia Conferencing	Creation of a multimedia conference and dynamic management of the participants involved
Address List Management	Management of address groups and management of members within a group, supporting add, delete and query operations.
Presence	Getting presence information about one or more users and registering presence for the same
Message Broadcast	Message sending to all the terminals in a specified geographical area
Geocoding	Getting geographical coordinates at which a terminal is located
Application-driven Quality of Service (QoS)	Dynamically change the quality of service available on end user network connections by third party applications
Device capabilities and configuration	Getting information about device capabilities and pushing device configuration to a device
Multimedia streaming control	Support of streaming multimedia
Multimedia multicast session management	Third party control on multicast sessions, their members and multimedia stream, and obtaining channel presence information
Content management	Uploading and consuming content into the network (or a third party content provider)
Policy	Policy provisioning and evaluation

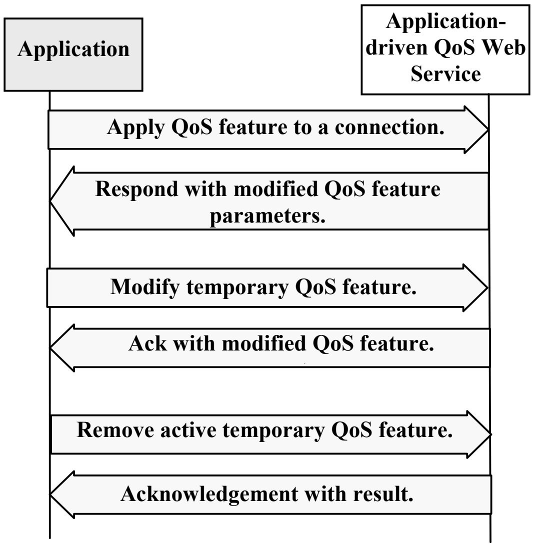

Application
Application-driven QoS Web Service
Apply QoS feature to a connection.
Respond with modified QoS feature parameters.
Modify temporary QoS feature.
Ack with modified QoS feature.
Remove active temporary QoS feature.
Acknowledgement with result.

Fig.28 The Parlay X application sets a temporary QoS feature to an end user connection

Fig.29 shows an example of where the Application registers its interest in receiving notifications of specific event types in the context of given end user. The notifications report network events that have occurred against end user active QoS feature(s).

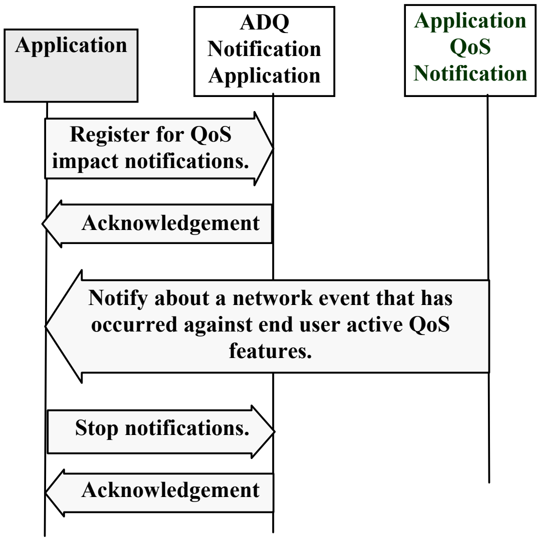

Application
ADQ Notification Application
Application QoS Notification
Register for QoS impact notifications.
Acknowledgement
Notify about a network event that has occurred against end user active QoS features.
Stop notifications.
Acknowledgement

Fig.29 The Parlay X application registers for QoS events and receives notifications

The "Application-driven Quality of Service" Parlay X Web Service is defined in [15].

C. *Policy Parlay X Web Service*

The "Policy" Web Service allows third party applications to manage policy information and to evaluate policies. Using the Web Service interfaces applications can personalize services according to their own preferences expressed as policies. On the other side, network operators and service providers can apply policy-based control on the access to their resources.

The "Policy" Web service provides four interfaces. The PolicyProvisioning interface is used for requesting the creation of a specified policy domain. It supports methods for policy domain management and policy rules management. The PolicyEvaluation interface is used to request an evaluation of a rule. The PolicyEvent-NotificationManager interface supports methods to subscribe for notifications about events and to request end of notifications. The PolicyEventNotification is used to deliver to the Applications with the event information when the monitored policy rule changes, e.g. when packet rates exceed.

Fig.30 shows an example, where an enterprise operator being a VPN client decides to cut down the expenses for the traffic generated by the employees over the weekends. To accomplish that the VPN client defines a policy allowing weekend packet rates twice lower than the ones over business days.

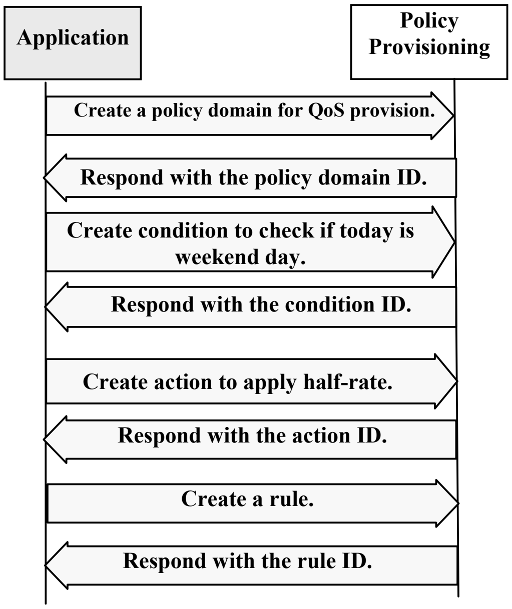

Application
Policy Provisioning
Create a policy domain for QoS provision.
Respond with the policy domain ID.
Create condition to check if today is weekend day.
Respond with the condition ID.
Create action to apply half-rate.
Respond with the action ID.
Create a rule.
Respond with the rule ID.

Fig.30 The Parlay X application creates a policy domain and policy rule

Fig.31 shows how to request the evaluation of a policy rule. The application creates first a signature in the domain before requesting the evaluation. The request for evaluation contains the name of signature.

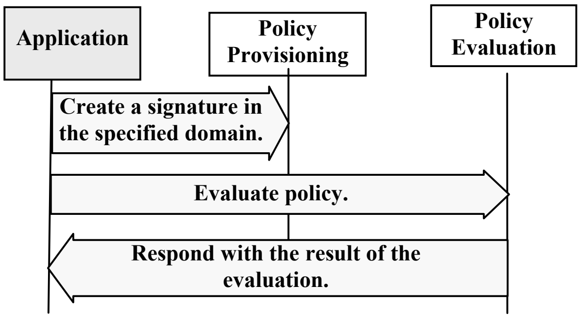

Application
Policy Provisioning
Policy Evaluation
Create a signature in the specified domain.
Evaluate policy.
Respond with the result of the evaluation.

Fig.31 The Parlay X application requests the evaluation of a policy rule

The Policy Parlay X Web Service is defined in [16].

VI. Conclusion

The purpose of resource management is to enable the telecommunication network to provide customers with the services they demand in a way that creates the greatest possible satisfaction and to enable operators to have these services provided at the lowest possible cost. Different mechanisms for resource management in IP-multimedia networks are defined. The access network and the transport network implement packet classification, scheduling and admission control. The operator uses mechanisms to assure that the negotiated QoS at SIP/SDP level is enforced at the access and transport network level. Resource reservation is realized in a coordinated manner with session establishment.

The opening network interfaces for third party software developers creates opportunities for provisioning of customer-oriented value-added services. The Open Service Access defined service architecture which abstracts applications from underlying network technology. The OSA Connectivity Manager interfaces enable the establishment, control and release of semi-permanent connections requested by telecommunications services such as virtual private networks. The OSA Policy Management interfaces allow network operators to host policy enabled service written by third party application service providers.

Parlay X interfaces provide abstraction of network functions by the use of Web Services. Application-driven Quality of Service Parlay X Web service and Policy Parlay X Web service may be used to create Parlay X applications for quality of service management in multimedia networks.

References

[1] Poikselka, M., Mayer, G., Khartabil H., & Niemi A.., *The IMS Multimedia Concepts and Services*, Wiley, 2008

[2] Rogelio Perea, *Internet Multimedia Communications Using SIP, A modern approach including Java practice*, Elsevier, 2008

[3] 3GPP TS 23.002 Network architecture, 2007

[4] 3GPP TS 23.203 v8.4.0, Policy and charging control architecture, 2009

[5] Alan Johnson, *SIP: Understanding the session Initiation Protocol*, Artech House, 2004

[6] 3GPP TS 23.218 V8.2.0, IP Multimedia (IM) session handling, IM call model, 2008

[7] ITU-T Y.1291, An architectural framework for support of Quality of Service in packet networks, 2006

[8] ETSI TS 183 017 v1.1.1, Resource and Admission Control: DIAMETER protocol for session based policy set-up information exchange between the Application Function (AF) and the Service Policy Decision Function (SPDF); Protocol specification

[9] 3GPP TS 23.107 v8.0.0, Quality of Service (QoS) concept and Architecture, 2008

[10] 3GPP TS 24.229 v5.21.0 IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP), 2008

[11] IETF RFC 2205 Braden, R., Zhang, L., Berson, Herzog, S., Jamin S.,. Resource ReSerVation Protocol (RSVP) – Version 1, Functional Specification, 1997

[12] Hu Hanrahan, Network Convergence, Services, Applications, Transport and Operations Support, Wiley, 2008

[13] 3GPP TS 23.198-10 v8.0.0, Open Service Access (OSA); Application Programming Interface (API); Part 10: Connectivity Manager Service Capability Feature (SCF)

[14] 3GPP TS 29.198-13 v7.0.0, Open Service Access (OSA); Application Programming Interface (API); Part 13: Policy Management Service Capability Feature (SCF)

[15] 3GPP TS 29.199-17 v8.0.0, Open Service Access (OSA); Parlay X Web Services; Part 17: Application-driven Quality of Service (QoS)

[16] 3GPP TS 29.199-22 v8.0.0, Open Service Access (OSA); Parlay X Web Services; Part 22: Policy

[17] Muslim Elkotob (2008), "Autonomic Resource Management in IEEE 800.11 Open Access networks", *http://epubl.ltu.se/1402-1757/ 2008/38/LTU-LIC-0838-SE.pdf*

Evelina Pencheva received her M.S. degree in mathematics at the University of Sofia, Bulgaria, and PhD degree in communications at Technical University of Sofia. Her current position is Associate Professor at the Faculty of Telecommunications. Her interests include next generation mobile applications and middleware platforms.

Ivaylo Atanasov received his M.S. degree in electronics at Technical University of Sofia, Bulgaria in 1992. He defended his PhD thesis in 2007 in the area of Telecommunications networks and systems. His current position is Assistant Professor at the Faculty of Telecommunications. His main research focus is development of open service platforms for next generation networks.