Journal of ELECTRICAL ENGINEERING, VOL. 54, NO. 9-10, 2003, 250–254

QUALITY OF SERVICE: A MECHANISM FOR EXPLICIT ACTIVATION OF IP SERVICES BASED ON RSVP

Dimitrios Kagklis — Christos Tsakiris — Nicolas Liampotis *

Since the beginning of 8Internet Protocol-based applications are the prevailing trend of the telecommunications market, but the path towards the "IP over everything" target is not unhampered. The main shortcoming of the IP protocol is its incapability of providing guaranteed Quality of Service (QoS). We propose a mechanism, which is based on the RSVP protocol, that provides the customer with means to request services with specific characteristics and the service provider with methods to supply these services with guaranteed QoS, as well as, to manage the network resources in order to support the requested levels of QoS.

K e y w o r d s: IP, QoS, Services, SLA-SLS, Signaling, RSVP

1 INTRODUCTION

Today telecommunications market is highly driven by IP-oriented applications and technologies. This is a completely different situation in respect of what happened in the past when almost all the traffic of telecommunications networks was voice. This tremendous proliferation of the Internet made the volume of data traffic close to that of voice traffic. As a result, a shift is occurring to the direction of technologies that initially were designed to serve merely data traffic but now they extend to employ other services such as voice, video or multimedia.

The IP protocol is the most popular to provide multimedia services. Standard IP provides what is called "best effort" service. However "best effort" can make no guarantees about when data will deliver, or how much it can deliver. In order to provide services with guaranteed QoS, firstly, at the customer side, there is a need for protocols that can provide Internet users with means to specify and activate IP services in unambiguous level of QoS and secondly, at the network side, mechanisms for providing differentiated high quality service management are required.

So far, Resource ReSerVation Protocol (RSVP) [1], which has been introduced by the Integrated Service (IntServ [2]) architecture, provides the mechanism to apportion network resources according to an application QoS request and subject to bandwidth management policy. On the other hand, Differentiated Services (DiffServ [3]) architecture classifies the network resources according to policy management criteria and ensures preferential treatment.

The current research status indicates that the solution for providing value added IP services to customers would be a combination of the IntServ and DiffServ architecture. The new architecture will supports the IntServ model for the customer side and the DiffServ model for the network side. The combination of the flexibility of the service provisioning through RSVP with the fine granularity of the IntServ model and the scalability offered by the DiffServ architecture is a promising solution. In this context, we propose a service management mechanism that performs aggregation of flows in the edge routers of the network while the customers and content providers make per flow network reservations outside the core network.

The main operation of the aforementioned mechanism is to manage the signalling messages, to map the service characteristics specified by the customer, to network parameters and to enforce the appropriate policies to the network in order to support the requested QoS levels [4]. The procedure for corresponding the customers' needs to network resources is based on the SLS Specification [5]. According to the type service, which is modelled with the XML language, the fields of the respective SLS specification parameters are filled.

Moreover, the reservation of resources for aggregated flows has been proposed in the context of DiffServ/Multi Protocol Label Switching (MPLS) architecture [6], as means for reducing significantly the signalling load and the state information stored at routers, while still providing the same QoS for real time flows. An extension to RSVP, the RSVP-TE [7] was recently defined to establish Label Switched Paths (LSPs) tunnels in MPLS networks. We adopted the RSVP-TE approach, and based on [8], we implemented a signalling protocol that uses the RSVP with policy extensions as a pure transport mechanism. The RSVP machinery is exploited for communication between peers and the activation signalling messages are encapsulated into the policy object of the RSVP messages [9].

The structure of this article is the following: In Section 2 the architecture of the proposed approach, as well as,

* National Technical University of Athens Telecommunications Lab., Dept. of Electrical & Computer Engineering Zografou Campus, Heroon Polytechniou 9, 157 73 Athens, Greece Email: kaglis, chrtsak, nliam @telecom.ntua.gr

First version of this paper was presented at SympoTIC ´ 03, 26-28 October 2003, Bratislava, Slovakia

ISSN 1335-3632

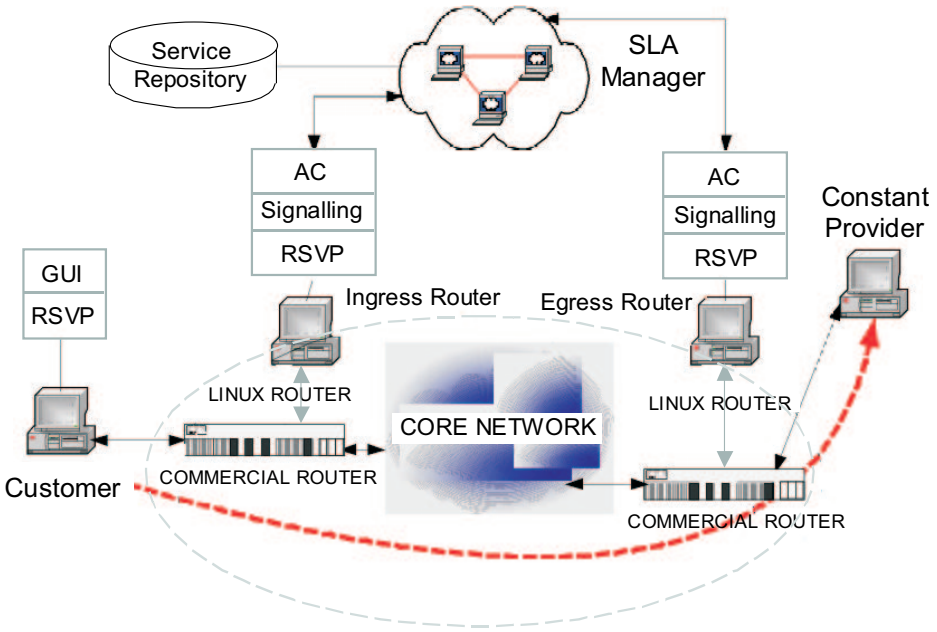

Fig. 1. Service Management Architecture

its components is described. In Section 3 a high level scenario, where interactions between these components take place, is further elaborated. In Section 4, the evaluation of the proposed model is presented. The article closes with the main conclusions including items for future work.

2 ARCHITECTURE

The proposed architecture provides the customer with means to request services with specific characteristics and the service provider with mechanisms to supply these services with guaranteed QoS, as well, as to manage the network resources in order to support the requested levels of QoS.

As depicted in the figure above our model performs management solely to the operation of the edge routers of the network by means of the ingress and the egress PC, each operating alongside the corresponding router. Taking into account the availability of bandwidth in the core network, the ingress and egress functionality focuses on the best utilization of the available bandwidth according to policies enforced to the edge routers. Moreover, taking into consideration the fact that the Service Provider (SP) makes use of open-source low cost solutions (Linux boxes) to manage the network, the operational cost of the SP is reduced significantly. In this approach, a SP that wishes to supply IP services does not really need an extended backbone network infrastructure but only requires leased broadband lines by the Network Provider (NP). The only drawback is that in cases of network failure the SP is dependant on the timely fault detection and resilience systems of the NP.

Finally, our model presupposes the support of the MPLS and the RSVP-TE protocols. The communication between customer, ingress and egress routers is performed through the RSVP protocol.

The aforementioned architecture can support multiple customers and multiple content providers. For simplicity reasons, in the rest of the article, we focus on the functionality of a single customer and a single content provider.

2.1 Components Description

In this subsection, the components and the functionality of the proposed architecture are described.

Graphical User Interface (GUI): The GUI provides the customer with a "service template" [10] that supplies information about the available services as well as a step-by-step walkthrough mechanism to select the service characteristics. The final requests as well as the customer's credentials are encapsulated in a XML document. We have to mention that the XML language has been used for the modelling of the services supported by the SP.

RSVP: The RSVP protocol is used as a pure transport protocol for the interchange of the XML documents, which describe the service requests, between the customer and the SP. For that reason, the RSVP sub-component has an additional implementation with regard to the standard RSVP, to support policy objects. This enhancement provides the protocol with the capability to transport the signalling messages, which encapsulate the XML documents.

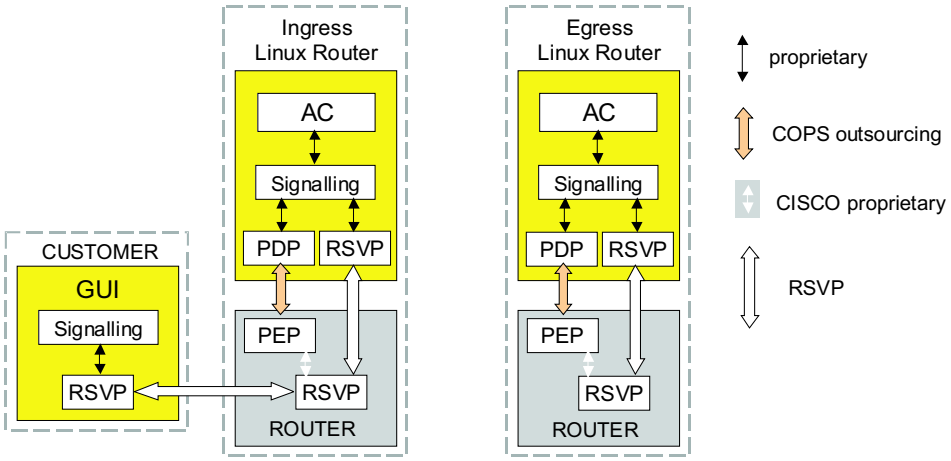

Fig. 2. Signalling mechanism

Signalling: The signalling component manages the activation signalling state machine, encapsulates the service activation requests to the appropriate RSVP messages and uses the RSVP machinery to communicate with its peers. We have to mention that the signalling sub-component opens only two sessions with the RSVP protocol so as to reject all other RSVP messages of the network, which are not complied with our model, and avoid the overhead of processing all the RSVP messages.

Admission Control: The main role of this component (AC in Fig. 1) is to maximize the number of admitted services and the QoS they enjoy, thus maximizing network utilization while at the same time preventing QoS degradation caused by overloading the network [11]. The AC component decides if a requested service can be best served according to the available resources of each traffic trunk. The concept of the traffic trunk comprises ingress-egress and QoS information for a certain service.

Service Manager: The Service Manager supports software mechanisms for mapping service requirements to network parameters, allocating resources, and storing the activated connections to a central repository [6]. It holds all the credentials of the authenticated customers registered to the specific SP in the customer repository of the central repository. Moreover, the Service Manager decides on the supported QoS Classes and is acquainted with the available traffic trunks. In the resource repository of our system, the available resources per traffic trunk of the network are stored.

The Service Manager evaluates the information stored in the central repository and taking into account the available resources, as well as the defined QoS classes and statistical information about the network usage in the past, it defines policies in an aggregated manner in order to best satisfy the customers demands. Mention that each policy includes parameters such as bandwidth, delay, jitter and packet loss. These policies may over-provision or over-subscribe the network resources according to class of service, available resources and other aspects such as time of day *etc.*

Finally, in the event of a service request that can be satisfied, the Service Manager sends the created policies to the ingress and egress, which in their turn enforce these policies to the edge routers of the network.

3 HIGH LEVEL END–TO–END SCENARIO

In this section, we present an end-to-end scenario. In the first paragraph, the service request is described through an end-to-end signalling mechanism while in the second paragraph the operations for the activation of the requested service, which are performed by the admission control along with the service manager components, are illustrated.

3.1 Operation Of Signalling Mechanism

As it has been mentioned above at the zero phase of the described scenario the signalling protocol initialises two RSVP sessions at all edge nodes, one for communication with the customer and one for communication between network edges.

The scenario starts at the time the customer wishes to receive a service (dashed line in Fig. 1) from the content provider. The customer fills the "service template" by using the supplied GUI block through which he provides his credentials, as well as, selects the characteristics of the service that best satisfy his needs. Once the procedure has finished, the GUI block passes the XML document that describes the service's characteristics to the customer side RSVP layer. The customer side propagates a PATH RSVP message to the ingress router of the network, which encapsulates the XML document in the RSVP policy object.

On the ingress router side, upon the reception of an RSVP message containing signalling information, the appropriate notification is launched to the signalling sub-component.

In order to overcome the lack of control in the RSVP messages on commercial routers, the COPS outsourcing facilities are used [12]. The COPS protocol regulates the treatment of the received RSVP messages but does not initiate RSVP sessions nor generates RSVP messages itself. Therefore, the COPS is used only to capture and respond to the RSVP PATH messages while the RSVP will be still the mechanism to request and receive replies from peer edges. Since the interface with the signalling subcomponent must be common with both types of routers (commercial and Linux), a common RSVP part must be build. The machinery of the signalling mechanism is shown better in Fig.2 and described by the following scenario [13].

The Policy Enforcement Point (PEP) of the COPS protocol (white arrow) handles The RSVP messages received in a router. The PEP forwards the received RSVP message to the Policy Decision Point (PDP) (wide shaded arrow). The PDP will extract the RSVP information and pass it as an event up-call to the signalling subcomponent, which in turn will appropriately notify the AC (black arrow). In order to communicate with the egress the signalling layer will trigger the RSVP protocol to send a new PATH message to the egress having the Router as the first hop. Upon confirmation of the request admission (described below in 3.2.), the PDP will be instructed to respond with a RESV message to the originally received PATH message.

Finally, when the customer wishes to terminate the service session then he issues a terminate signal which is forwarded to the ingress and egress routers as PATH TEAR RSVP message so as to inform the SP of the service termination and de-allocate the reserved resources.

3.2 Service Manager & Admission Control Operation

At the zero phase of the described scenario the Service Ma nager (SM) component initiates the Customer repository, which holds information about the SP's registered customers. Moreover the SM initiates a) the Network repository in which the location of the available content and service servers, b) the supported QoS classes (*eg* EF, AF, *etc.*) as well as c) the traffic trunks, which specify the ingress and egress router topological information in combination with a QoS class. Finally, the Resource repository and the Service Session repository are initiated which hold the available network resources per traffic trunk and the current active connection respectively.

On the ingress router side, the Admission Control component, upon reception of a signalling message indicating a new service request, validates the received message and forwards it to the Service Manager. Then the SM maps the service requirements encapsulated in the XML document to network parameters based on SLS specification. For each service session request and its specific characteristics, there is a unique correlation to SLS specification parameters according to the location of the requested server, the desired bandwidth and the tolerance of the service application to the level of delay and congestion of the network.

Next, the Admission Control authorizses the customer and decides whether the service can be efficiently provided by the network infrastructure from the customer location to the ingress router's location. Firstly, the service is assigned with the QoS class that best fits to its requirements. Secondly, according to the location of the requested content server the Admission Control of the ingress side will decide the service corresponds to which traffic trunk. Finally, the availability of the network resources is examined by querying the Resource repository.

Upon succession, a new RSVP message including the customer's original XML document is propagated from the ingress to the egress router waiting for confirmation. On the egress router side, the procedure performed is similar to the one described for the ingress router side. If the service can be satisfied, a confirmation message is returned. Then the Admission Control of the ingress router informs the Service Manager of the succession of the service session request. In this case, the Service Manager enforces the policy to both network edge routers, through the ingress and egress respectively. At this point, the customer is capable of receiving the service he requested. The traffic engineering mechanism applied to the packet flow of the activated service is out of scope of this article and will therefore not be presented here.

4 EVALUATION OF PROPOSED MECHANISM

Our model has been tested successfully in the test bed of the Multimedia Laboratories of the Research Department of OTE. The implementation of the proposed architecture was carried out in a distributed way (component platform) using the Java technology as the main programming language. The implemented code was "running" on Linux PCs and we have used two Cisco routers of the 3600 series attached to the customer, the ingress Linux PC and the egress Linux PC. As core network, we have used a Cisco router of 7500 series. We have performed integration of our software subcomponents and interoperability among them and the Cisco routers. The test-bed supported MPLS and the Cisco routers had the Open Short Path First (OSPF) routing protocol configured.

We avoided to introduce new protocols and based on existing protocols and technologies. The enhancements and the protocols we have implemented were designed in order to be compliant with existing network status and IP network protocols and standards (Cisco routers, IETF standards). As we used the RSVP protocol as a pure transport protocol, the only thing that mattered was the interoperability of the enhanced RSVP implementation of the introduced model with the RSVP "daemons" of the Cisco "black" boxes. The Integration of the RSVP with the COPS protocol was a key-point for the success of our mechanism.

Moreover, the proposed mechanism operates only on the edge routers of a backbone network; therefore, there can be no cumulative comparison between the introduced enhanced RSVP-TE implementation and the RSVP [1] protocol. In more detail, in an extended core network of N number of routers the RSVP needs a per hop reservation in order to have an end-to-end reserved channel while in our model only the reservations in the ingress and egress routers are needed.

Furthermore, we modelled the network parameters and based on SLS specification [5] and implemented a graphical user interface (GUI) with which a customer can specify the level of QoS of a service described within a SLA. This SLA is an XML document that is sent to the service provider via the implemented enhanced RSVP-TE protocol through the method that was above further elaborated.

Finally, the XML document, which specifies the service characteristics, provides the ISP with means for Authentication Authorization and Accounting. If the customer used only the RSVP protocol for service activation the ISP could never know at any time the identity of customers and the utilization of its network resources.

CONCLUSIONS

This article gives an overview of a novel service management framework, which allows the provisioning of guaranteed QoS IP services with signalling mechanisms. The proposed model is a low cost solution based on existing technologies. It offers the customer with means of easily selecting his service requirements while the ISP is capable of managing effectively the provided services. It tries to introduce a model for the combination of the flexibility of the service provisioning through RSVP with the fine granularity of the IntServ architecture and the scalability offered by the DiffServ architecture.

In future work we intend to evaluate the performance of our model in a more extended backbone network and examine the behaviour of the mechanism in cases of multiple service activation requests and analyse the results especially when our model fails to accommodate the customer's request.

Acknowledgements

The authors would like to thank all TEQUILA colleagues who have also contributed to the ideas presented here.

References

[1] R. BRADEN, et al: Resource ReSerVation protocol (RSVP) - version 1 functional specification, RFC 2205, September 1997.

[2] R. BRADEN et al: Integrated Services in the Internet Architecture: an Overview, RFC 1633, June 1994..

[3] S. BLAKE et al: An Architecture for Differentiated Services, RFC 2475, December 1998.

[4] IST-TEQUILA Homepage, <http://www.ist-tequila.org>.

[5] D. GODERIS et al: Service Level Specification semantics, parameters and negotiation requirements, Internet Draft, Internet Engineering Task Force, June 2001.

[6] P. TRIMINTZIOS et al: A Management and Control Architecture for Providing IP Differentiated Services in MPLS-based Networks, IEEE Communications Magazine, Vol.39, No.5, May 2001.

[7] D. AWDUCHE et al: RSVP-TE: Extension to RSVP for LSP Tunnels, RFC 3209, December 2001.

[8] RSVP-TE daemon for DiffServ over MPLS under Linux, <http: dsmpls.atlantis.rug.ac.be>.

[9] D. KAGKLIS et al: Approach for Activation of IP Services with Guaranteed QoS Using Signaling Mechanisms, Symposium on Trends in Communications, (SympoTIC), Bratislava, Slovakia, October 2003.

[10] IST-CADENUS Homepage, <http://www.cadenus.org>.

[11] E. MYKONIATI et al: Admission Control for Providing QoS in DiffServ IP Networks: The TEQUILA Approach, IEEE Communications Magazine **41** No. 1, January (2003).

[12] S. HERZOG et al: COPS usage for RSVP", RFC 2749, January 2000.

[13] D. KAGKLIS et al: Architecture for the Creation of Service Level Agreements and Activation of IP Added Value Services, IEEE 7th International Conference on Telecommunications, ConTEL, Zagreb, Croatia, June 2003.

Dimitrios Kagklis (PhD Candidate) was born in 1976. He received a diploma in electrical and computer engineering in 1999 and an MsC on techno-economic systems in 2001, from the National Technical University of Athens, Greece. From 1999 until now, he works as a research associate and since 2001; he is a PhD Candidate at the Telecommunication Laboratory of the National Technical University of Athens. He has been involved in the PRO-3, TEQUILA and AV-PACK IST, P-919 Eurescom and in several Greek research projects. His main research interests include traffic engineering, IP QoS provisioning, service management and QoS aware admission control.

Christos Tsakiris (MSc student) was born in 1978. He received a diploma in electrical and computer engineering in 2001 from the National Technical University of Athens, Greece. In 2001, his diploma thesis has been awarded by TELESTET- HELLAS as one of the best three on mobile networks. From 2001 until now, he works as a research associate at the Telecommunication Laboratory of the National Technical University of Athens, where he is also about to finish his MSc on techno-economic systems. He has been involved in the TEQUILA IST and in a couple of Greek research projects. His main research interests include service modelling, service delivery, network dimensioning and service management.

Nicolas Liampotis (undergraduate student) was born in 1980. He is undergraduate student in the National Technical University of Athens. He is expected to finish his studies in 2005. Currently, he works as a network administrator and a research assistant at the Telecommunication Laboratory of the National Technical University of Athens. He has been involved in the TEQUILA IST since 2001 and in a couple of Greek research projects. His research activity include working on XML-based modelling of QoS-based IP connectivity services and service management issues. His main research interests include service modelling, traffic engineering, and network dimensioning, service as well as network management and QoS-aware admission control.